2020

Strategic Competition and Escalation Management in the 21st Century: Russian Hybrid Warfare and China's Rise

Raymond L. Reilly III
University of Denver

Strategic Competition and Escalation Management in the 21st Century: Russian Hybrid Warfare and China's Rise

_____

A Thesis

Presented to

the Faculty of the Josef Korbel School of International Studies

University of Denver

_____

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

_____

by

Raymond L. Reilly III

June 2020

Advisor: Dr. David Goldfischer

Author: Raymond L. Reilly III
Title: Strategic Competition and Escalation Management in the 21st Century: Russian Hybrid Warfare and China's Rise
Advisor: Dr. David Goldfischer
Degree Date: June 2020

Abstract

The U.S. National Security Strategy (NSS) and the unclassified version of the U.S. National Defense Strategy (NDS) both focus on China and Russia as preeminent challenges for the United States. The NDS states specifically, "Long-term strategic competitions with China and Russia are the principal priorities for the Department [of Defense]."[1] This paper focuses on the strategic challenges that these two nations pose and provides recommendations for U.S. strategy and policy. Globalization and the rapid advancement of technology has changed the utility of force in the 21st century. The utility of force has evolved, resulting in a shift in the character of war. This shift entails an increased focus on methods of force mainly below the threshold of traditional armed great power conflict. In order to preserve a stable international order, the U.S. needs strategies and polices that adapt to the new threat environment. In particular the United States should: (1) Concurrently build defensive capabilities and adopt a strong and public policy of deterrence to counter current and emerging hybrid, gray-zone, and advanced technological threats. (2) Renew dedication to longer-term interests and favor negotiated solutions—including pursuing norms and agreements on emerging conflict-relevant technologies—to counter the growing risk of miscalculation and escalation from gray-zone provocations (most notably in the cyber domain). (3) Increase domestic resilience

[1] Mattis, J. (2018, January 19). Summary of the National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

by strengthening the electoral system, building stronger public-private partnerships, and working with the international community to increase attribution in the cyber domain. (4) Ratify the United Nations Convention on the Law of the Sea and provide additional funding for initiatives in the Indo-Pacific. (5) Strongly defend the status quo with Taiwan and in the South China Sea but, after increasing U.S. strategic involvement in the region, lead and pursue negotiations on more permanent solutions.

Table of Contents

Introduction

U.S. national interests and priorities can and will evolve, especially with changing administrations. In the 2017 U.S. National Security Strategy, the Trump Administration laid out the nation's four vital national interests, called the "four pillars": Protect the homeland, the American people, and the American way of life; promote American prosperity; preserve peace through strength; and advance American influence.[2] Since the Cold War, the United States has also traditionally viewed a strong North Atlantic Treaty Organization (NATO), strong U.S. led liberal institutions worldwide, and flourishing democratic governance as being vital to the interests of the United States. All of these interests must be considered when building a strategy.

> Long-term strategic competitions with China and Russia are the principal priorities for the Department, and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future.[3] – Unclassified Summary of the 2018 U.S. National Defense Strategy

The 21st century, has been marked by an evolving and increasingly complex threat environment. According to the 2018 Worldwide Threat Assessment of the U.S. Intelligence Community, "[t]he risk of interstate conflict, including among great powers,

---

[2] United States, The White House. (2017, December). *National Security Strategy of the United States of America*. Retrieved April 16, 2019, from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[3] Mattis, J. (2018, January 19). Summary of the National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

is higher than at any time since the end of the Cold War."[4] Although the risk of conflict is increasing, the environment in which conflict occurs is heavily impacted by nuclear weapons, escalation management, and a rapidly evolving technological environment. These factors have led nations to significantly limit and change their use of force; while there is no shortage of conflict globally, the forms that conflict has taken have shifted to more non-traditional means. Globalization and the rapid advancement of technology has changed great power politics and the utility of force. This change demands new strategies and policies, if the U.S. led international order is to thrive. To describe empirically how the utility of force has changed, this thesis examines some recent conflicts, threats, and interactions involving Russia, China, and the United States. Key topics include hybrid warfare, election interference, certain cyber events, and the tense situation in the South China Sea. Following the analyses, policy recommendations for the United States are made.

Russian and Chinese actions have catalyzed the evolution of geopolitics in Eurasia and increasingly threatened U.S. interests in the region. Russia is a major threat to the United States and is developing new weapons and technologies to threaten U.S. assets both internationally and in outer space. Furthermore, Russia's use of hybrid warfare and election interference raises major domestic concerns and challenges. Russia currently poses the greatest military threat to the United States but has less potential for growth and long-term strategic disruption when compared to China. Thus, a more

[4] Coats, Daniel R. "Worldwide Threat Assessment of the Intelligence Community." *ODNI*, Office of the Director of National Intelligence, 13 Feb. 2018, www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

traditional policy of strong deterrence and strategic messaging is recommended—especially with regard to cyber threats and interference in essential democratic processes.

One of the greatest challenges for the United States in the 21st Century will be adapting to and shaping the evolving international order in a way that satisfies and favors U.S. equities, while also addressing the core interests of the Communist Party of China—to encourage further assimilation into the current order. China has more recently become a major threat to the interests of the United States and has grown and expanded its influence not only in the Eurasian region, but globally. It has high potential for continued growth and expansion both economically and militarily. China has invested a large portion of its wealth in new technology and military capabilities and has continued to steal cutting-edge military advances and technology from other countries—particularly the United States. China's domestic aircraft carrier program is eventually expected to launch multiple modern aircraft carriers, including one that is similar in size and capability to the newest U.S. carrier class—the Gerald R. Ford. This will impact the balance of power and geopolitics of the region and will continue to afford China more military leverage. In addition to the use of cyber capacities against the United States, China has also been developing and testing various outer space and anti-satellite capabilities that threaten U.S. assets.

Growth in Chinese influence and power is inevitable, and U.S. strategy and policy must take this into greater account. The U.S. response to China should be different than the response to Russia. If strong Chinese growth continues, sooner or later their concerns in Eurasia—as well as their concerns regarding the current international order as a whole—will have to be adequately addressed. The United States must create a dialogue

with China toward determining what it would take for China to become a willing and more productive member of the current international order—instead of a revisionist power trying to supplant it. If this is to be accomplished, major powers benefiting from the current order must be willing to make significant concessions of value. Additionally, if concessions are to be made, it is in the best interest of the status quo powers to make them sooner rather than later. As China continues to grow, it will gain more leverage and will demand greater concessions—making reaching an agreement more difficult. Thus, it is in the best interest of the United States to prioritize cooperation with Beijing now, while also managing Chinese growth and ensuring that China becomes a constructive member of the current international order.

That goal includes promoting the rule of international law and the U.S. should ratify the United Nations Convention on the Law of the Seas (UNCLOS). Finally, the U.S. must remain a strong and continuing presence in the Indo-Pacific. It is in the United States' best interest to provide more funding for political, military, and economic initiatives in the region and to assure allies and partners in the region of its continued commitment. These actions will help ensure that the U.S. will be negotiating from a position of strength and will be able to resolutely respond if China commits fully to fighting against the rule of law and current international order.

The Utility of Force in the 21st Century

The utility of force, in the sense of direct physical fighting, has been reduced in the 21st century, making war between major powers' militaries highly unlikely. Defense and deterrence are still essential and necessary, but the importance has shifted from physical territorial control over an adversary to political control and influence by other means. New capabilities and advancements in technology have changed the context and shifted the traditional utility of force—changing the character of war. The U.S. Department of Defense has even recognized this in the most recent unclassified version of the National Defense Strategy stating that the "security environment is also affected by *rapid technological advancements and the changing character of war*."[5]

The invention of nuclear weapons and their proliferation has drastically increased the escalatory risks of waging political violence against others—especially against a nuclear power. Additionally, even if a nation is not a nuclear power, large scale political violence against another nation has still become riskier. The constant threat of an external power deciding that it wants to impact the outcome of a conflict increases the likelihood of unexpected escalation that could fundamentally change the conflict. If a great power decides that it is in its best interest for one side to win a conflict—or simply that it did not

[5] Mattis, J. (2018, January 19). Summary of the National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

want one or any of the sides to emerge victorious—they have multiple ways to change the dynamic of the conflict, through direct force, covert action, cyberattacks, military assistance, economic sanctions, and/or political pressure. The addition of cyberwarfare and new technologies in recent years have continually added more means below large scale armed conflict and it is likely that this trend will continue. As more of these capabilities are employed successfully, research and development will remain a priority.

Investing in militaries and building the capabilities to use force is still necessary to ensure that the escalatory ladder creates ample risk to continue to be a strong deterrent. For example, a nuclear power need not explicitly threaten the use of nuclear weapons to achieve a deterrent effect. Simply having the capability to mutually assure destruction (MAD) is enough to fundamentally increase the escalatory risk of engaging in any type of conflict. This is why escalation management is so critical in the 21st century. There will always be an *us* vs. *them* mentality somewhere in the world. Therefore, there will always be an actual or potential adversary. How nations and groups plan and strategize for interactions with their adversaries has evolved to require extreme caution with regard to escalation. Whether considering a nuclear attack, armed conflict, use of cyber capabilities, espionage, space weaponization, predatory economics or even election influence, extreme caution and due regard to escalation risk must always be taken to formulate an effective strategy in the 21st century. While limited war and MAD are not new topics, the rapid growth and development of new technologies has led to additional challenges that are less black and white. Cyberweapons, artificial intelligence, militarization of space, and various other technological advancements in warfare have

made escalation management more complex, but no less important. Without a proper escalation management strategy, plans will not survive first contact with a major power.

In terms of complexity, recent technological advances challenge traditional thinking of the use and utility of force. For example, a cyberweapon that causes physical damage to a nation's critical infrastructure that impacts national security, or even a population's safety, must still be deemed as a use of force. However, cyber-attacks on servers to steal information may seem more similar to traditional espionage than to force for some—even if this attack causes some property, software, or monetary damage. The difficulty is distinguishing between types of attacks within this domain that all may be classified differently by different people, nations, or institutions—especially when there is an infinite number of possible variations. Thus, even if all nations wanted cyber arms control, creating effective agreements or laws limiting this domain would likely prove incredibly difficult, if not impossible. Therefore, nations are left to make difficult and complex judgements regarding both offense and defense in this domain with due regard to escalation management—especially, when the adversarial nation or actor has developed either actual nuclear capability or a nuclear-like technological capability. Additionally, it requires cyber actors (both state and non-state) to consider hybrid ramifications of even small attacks, counterattacks, and escalations both within and outside of the cyber domain. Each actor making these rapid and complex decisions in this domain leaves significant room for dangerous miscalculation—especially in a domain where attribution can prove difficult.

There are strong incentives to limit the use of force, however there is still circumstantial utility. The use of small and specialized forces to conduct covert action in

support of groups and nations with similar interests still plays a significant role. This can achieve national policy objectives with minimal escalatory risk and, in some cases, can even be done while hiding the hand of the actors involved. Some examples include covert action, counterterrorism operations, intra-state conflict, and proxy wars. Actors have been able to effectively utilize an amount of force that is limited enough to not provoke a major escalation, but still achieves their main political objectives.

Given the limited utility of force, states are incentivized to find utility elsewhere to gain greater power, influence, and control over outcomes. The utility of economics in the 21st century has been a major focus for many actors—but has been especially evident for China. The Chinese government has made it clear that they intend to change the status quo and create a region and world in which China holds a stronger and more influential position in the global order. With the understanding of today's limited utility of force, China has been playing a long-term economic strategy to achieve great power status and increase its global influence.[6] It has been capitalizing on a large workforce, dedicating significant resources to foreign investments, and using its rapidly growing economy to become a major influencer in the region. "China's double-digit economic growth has slowed recently, but it served to fund several successive defense modernization Five-Year Plans".[7]

---

[6] Mastro, Oriana Skylar. "The Stealth Superpower." *Foreign Affairs*, Foreign Affairs Magazine, 4 Feb. 2019, www.foreignaffairs.com/articles/china/china-plan-rule-asia.

[7] United States, Defense Intelligence Agency. (2019, January 3). *China Military Power*. Retrieved April 16, 2019, from https://www.dia.mil/Portals/27/Documents/News/Military Power Publications/China_Military_Power_FINAL_5MB_20190103.pdf

Additionally, China has realized it is much cheaper and faster to steal cutting edge technologies from other countries than to dedicate vast amounts of resources on developing them from scratch. It is clear that the Peoples Liberation Army and its Naval branch (PLAN) are growing and modernizing at a rapid pace—especially with regard to its aircraft carrier program.[8] Having a modern navy with similar capabilities to the United States automatically provides status, influence, and deterrence—even without any explicit threat—which can shift the geopolitical situation without the actual use of force.

The ability to modernize and grow the military this rapidly is a product of actions taken below the threshold of armed conflict. The strategy has included economic priorities, cyber operations, and effective intelligence operations. According to the 2017 National Security Strategy of the United States,

> Every year, competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars. Stealing proprietary technology and early-stage ideas allows competitors to unfairly tap into the innovation of free societies.[9]

This has become a significant way for adversaries to achieve political goals without using force and without major risk.

Russia, in some instances, has taken an approach that involves greater risk of escalation than other actors, but this is a product of Russia's less fortunate geopolitical

---

[8] Mizokami, Kyle. "China Could Have 4 Aircraft Carriers by 2022: Should the Navy Be Worried?" *The National Interest*, The Center for the National Interest, 12 Sept. 2018, nationalinterest.org/blog/buzz/china-could-have-4-aircraft-carriers-2022-should-navy-be-worried-31077.

[9] United States, The White House. (2017, December). *National Security Strategy of the United States of America*. Retrieved April 16, 2019, from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

and economic situation. The Russian economy is extremely dependent on natural resource production (mainly oil and gas) and does not have the Chinese luxury of playing a long-term strategy that is primarily focused on economics. The Russian mindset, and subsequently its strategy, is based heavily on a historical pattern of defeats and a desire to gain back some of its previous Soviet glory. This mindset combined with President Putin's previous career as a KGB officer places a premium on military strength; however, Putin still understands the limited utility of force and utilizes restraint.

As seen in Ukraine, military deception and focused information operations were utilized to sow confusion and make reaction and further escalation extremely difficult and delayed. This was what created the time and space for the main objectives to be achieved rapidly, while also deterring a major escalatory response by the West. Putin also understood that he needed to limit his campaign to Crimea and eastern Ukraine. A full military incursion that was meant to completely take over the Ukrainian state would have required significantly more force, resources, and time. The elements of surprise and confusion that were created by the advanced information operations and relatively limited use of force would have eventually been lost—and the possibility of major escalation by the U.S. and other states would have increased substantially. While taking over Sevastopol was an important military objective, making a move on Ukraine was motivative by geopolitical strategy.

NATO-Russia relations in Eurasia can be described as geopolitical chess. Russian military strength and advanced technological capabilities are important for attempting to deter NATO enlargement near its borders. On March 27, 2020, North Macedonia became

the 30th member of the Alliance.[10] Although North Macedonia is not geographically close to Russia, it is evidence that NATO is still enlarging and "[a]t the 2008 Bucharest Summit, the Allies agreed that Georgia and Ukraine would become members of NATO in the future."[11] Russia is appropriately concerned that NATO enlargement will decrease Russia's relative power and influence both in the economic and political realms. Additionally, NATO enlargement in Eurasia decreases and, in some cases, eliminates buffer zones that Russia views as important. Even if assuming complete Russian confidence that NATO poses no offensive military threat, it still has reasons to oppose NATO enlargement. As more neighboring states become members of NATO and receive security guarantees, the amount of actions or moves Russia can take without invoking Article 5 or running into significant political opposition become more limited. Conversely, NATO and the U.S. gain more freedom of action as NATO expands, especially when expansion is linked to a widening zone of Western economic and political integration and growth. That linkage between military expansion and economic and political power helps to explain why Russia tries to expand where it can and weaken the U.S. and NATO whenever there is an opportunity. For example, in addition to its actions in Ukraine and Syria, Russia has been expanding into the Arctic militarily.[12] The

[10] NATO. (2020, March 30). North Macedonia's flag raised at NATO Headquarters, following accession to NATO. Retrieved April 22, 2020, from https://www.nato.int/cps/en/natohq/news_174648.htm?selectedLocale=en

[11] NATO. (2020, April 7). Enlargement. Retrieved April 22, 2020, from https://www.nato.int/cps/en/natolive/topics_49212.htm

[12] Gramer, R. (2019, June 1). Here's What Russia's Military Build-Up in the Arctic Looks Like. Retrieved April 3, 2020, from https://foreignpolicy.com/2017/01/25/heres-what-russias-military-build-up-in-the-arctic-looks-like-trump-oil-military-high-north-infographic-map/

northern approach is not only the closest and most likely route that either the U.S. or Russia would take for an attack, but also is home to vast natural resources including oil and natural gas.

Russian economic expansion and growth is limited relative to other great powers. Therefore, the development and use of various means just below the threshold of armed great-power conflict have been a top priority for the Russians. Due to Russia's geopolitical and economic situation, the Russian policy accepts more risk and they are more willing to test out gray-zone/hybrid capabilities. However, the Russian's still take great caution to stay below the threshold of provoking a major escalatory response from their adversaries. General O'Shaugnessy, the Commander of U.S. Northern Command (NORTHCOM) and North American Aerospace Defense Command (NORAD) has spoken publicly to Congress about this threat from Russia and other adversaries:

> [K]ey adversaries have demonstrated patterns of behavior that indicate they currently have the capability, capacity, and intent to hold our homeland at significant risk below the threshold of nuclear war. Eroding military advantage is undermining our ability to detect threats, defeat attacks, and therefore deter aggression against the homeland. This is emboldening competitors and adversaries to challenge us at home, holding at risk our people, our critical infrastructure, and our ability to project power forward.[13]

Although Russia has been more aggressive and has risked greater escalation, the strategy has largely been effective—as the U.S. has not significantly escalated. Russia is clearly testing the boundaries to try to determine exactly how limited the use of force is in the 21st century. It is clear that the U.S. is capable of escalating but has so far been

[13] Statement of General Terrence J. O'Shaughnessy Before the House Armed Services Committee Subcommittee on Strategic Forces. Terrence, O. S. J. (2020, March 12). Retrieved April 22, 2020, from https://docs.house.gov/meetings/AS/AS29/20200312/110671/HHRG-116-AS29-Wstate-OShaughnessyT-20200312.pdf

unwilling. For the current administration, the risks and costs up to this point have apparently outweighed the benefits of significant escalation by the U.S. If the United States was willing to escalate through retaliation and effectively communicated this willingness, then the Russian's would likely recalculate and further bound and limit their operations. However, the Russians are currently willing to wade into unexplored waters and find out just how far they can go without significant consequence—in other words, figuring out what actions do and don't cause significant escalation. The Russians are trying to determine exactly where that threshold (or line) actually is in the current geopolitical context. However, this is not only a probing/scouting maneuver, but also is a mission that has "battle" tested capabilities and achieved significant effects on its targets—as evidenced by the 2017 U.S. intelligence community assessment on Russian election interference.[14]

There is currently a limited utility of force and it is very likely to continue into the near future; however, if there is fundamental change in the current conditions, the utility of force could exponentially increase. Some events or circumstances that could potentially cause a resurgence in the utility of force are listed and described below:

Pivotal Discoveries or Inventions: (either on Earth or in outer space)	Fundamental Change in Great Power Relationships: (possibly an even closer Russia/China relationship)	Extreme Impacts Stemming from a Significant Change in Climate	Development of an Extreme Cyber Capabilities/Artificial intelligence Gap: (where one nation or group holds a vast and consequential comparative advantage over all others)

[14] Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." *Assessing Russian Activities and Intentions in Recent US Elections*, ODNI, 6 Jan. 2017. www.dni.gov/files/documents/ICA_2017_01.pdf.

If any of these or other major shifts—like regime change—occur, then global geopolitics could change fundamentally. These examples and others would result in significant change in actors' cost-benefit analyses. If a country is suffering from major famine, for example, the survivability of the state could be threatened. In this instance, the Hobbesian state of nature could kick in and make states and people act in ways they would not have otherwise. The risk of escalation and the cost of using more force may actually become worth the potential benefits of achieving certain political or physical gains through force. Caution would still be necessary—because ultimately getting nuked would not increase survival chances—but pushing the boundaries without breaching the nuclear threshold may certainly be more favorable when a state or its people are fighting for survival.

In the current state of international relations and security, there is a limited utility of force; however, the degree to which force continues to be limited in the future is still in question. This will be determined by many factors, but escalation management will continue to play an important role regardless. As we have seen with globalization and the invention of the internet, new technologies have the potential to rapidly transform the economic and security environments. Therefore, in order to improve the likelihood of long-term success, competing great powers must have a strategy to remain vigilant in retaining various capabilities in many different areas in order to have the ability to continuously adapt to challenges in the 21st century and beyond. In today's rapidly evolving global environment, adaptability is absolutely critical to the long-term success of any international order. A static system that continually fights change at every turn is a

system that is destined for failure, but a system that adapts and effectively manages change will thrive.

States wishing to either remain great or continue gaining influence must have the ability to pivot when necessary to meet the demands of a changing world. A very capable diplomatic arm combined with a strong military and thriving economy will better position a state to be able to adapt quickly to threats while also attracting partners. Economic strength not only provides the resources necessary to effectively respond to threats, but also the resources to retain capabilities and develop new ones. A strong economy also contributes to increased morale of citizens: as Napoleon Bonaparte said, morale is to the physical as three to one.

Globalization and the rapid advancement of technological capabilities have increased the complexity of deterrence, defense, warfighting, and escalation management. Major advancements in cyberwarfare, space, artificial intelligence, and nuclear delivery systems—like hypersonic glide vehicles—have expanded the traditional nuclear concept of mutually assured destruction and the retaliatory risks of using force. Achieving greater power and influence today, due to the increase in escalatory risk and cost, has mainly (but not entirely) shifted the means of conflict to those which are typically below the threshold of armed conflict. The current state of the world contains the necessary conditions for these limitations of the utility of force. However, as new technologies emerge, the utility of force will also continue to evolve. The United States must be properly prepared and positioned to adapt to the future environment. As stated clearly in the 2018 National Defense Strategy, Russia and China must be the primary strategic priorities for the United States—due to their current and future threat to U.S.

security and prosperity.[15] The next section addresses U.S. relations and policy regarding Russia and is followed by a section on China.

[15] Mattis, J. (2018, January 19). Summary of the National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

U.S.-Russian Relations and Hybrid Warfare

"The risk of interstate conflict, including among great powers, is higher than at any time since the end of the Cold War."[16]
—2018 Worldwide Threat Assessment of the Intelligence Community

In modern warfare, new technologies and strategies have created an evolution of the manner in which conflict occurs. The terms hybrid warfare, new generation warfare, and others have been used to describe warfare which has more than one facet. These facets include conventional, unconventional, cyber, and influence campaigns—such as disinformation spread on social media and targeted election interference. Since Russia is a major power, and historically has been an adversary of the United States, understanding Russian actions and methods of conflict is essential for the Homeland Defense of the United States.

Russia has used hybrid tactics within the U.S. and in conflicts abroad. Russia has utilized many different aspects of hybrid warfare, especially in the military realm. Regarding modern-day hybrid tactics abroad, the following section uses the Ukrainian conflict as a case study. The 2017 National Security Strategy of the United States describes some Russian views and threats:

> Russia aims to weaken U.S. influence in the world and divide us from our allies and partners. Russia views the North Atlantic Treaty Organization (NATO) and European

[16] Coats, Daniel R. "Worldwide Threat Assessment of the Intelligence Community." *ODNI*, Office of the Director of National Intelligence, 13 Feb. 2018, www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

> Union (EU) as threats. Russia is investing in new military capabilities, including nuclear systems that remain the most significant existential threat to the United States, and in destabilizing cyber capabilities. Through modernized forms of subversive tactics, Russia interferes in the domestic political affairs of countries around the world. The combination of Russian ambition and growing military capabilities creates an unstable frontier in Eurasia, where the risk of conflict due to Russian miscalculation is growing.[17]

The constant threats from Russia are still evolving and the U.S. response must be adaptive, vigilant, and proactive. This section evaluates the hybrid threat from Russia and makes policy recommendations for threat mitigation.

It is essential to define the scope of the threat Russia poses to its adversaries and enemies. Christopher Chivvis from the Rand Corporation, testifying before the House of Representatives' Committee on Armed Services described the scope of Russian hybrid warfare:

> As used today in reference to Russia, "hybrid warfare" refers to Moscow's use of a broad range of subversive instruments, many of which are nonmilitary, to further Russian national interests. Moscow seeks to use hybrid warfare to ensure compliance on a number of specific policy questions; to divide and weaken NATO; to subvert pro-Western governments; to create pretexts for war; to annex territory; and to ensure access to European markets on its own terms.[18]

It is important to note that this warfare not only includes tactics taken on the ground in physical military combat, but also has a very large nonmilitary component. The following section focuses on the components of cyber, information operations, psychological operations, and election interference.

---

[17] United States, The White House. (2017, December). *National Security Strategy of the United States of America*. Retrieved April 16, 2019, from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[18] Chivvis, Christopher S. *Understanding Russian "Hybrid Warfare."* RAND Corporation, 22 Mar. 2017, www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

Russia's War on U.S. Democracy

The great power and liberal democratic ideology of the U.S. will always create adversaries like Russia. Timothy Snyder, in his book *The Road to Unfreedom*, uses the term "strategic relativism" to describes the Russian foreign policy goal of making others weaker in order to benefit the Russian position geopolitically. If one of the strongest actors in the world and in Europe/Eurasia (the U.S.) is weakened, then Russia will gain relative strength. Snyder also argues that Russia is very limited in the amount of absolute strength that it can attain, which is why the relative gains are so imperative.[19]

This argument helps to explain one significant reason why Russia has taken to Hybrid Warfare tactics—and more specifically, cyber and information warfare aimed at the very foundation of the U.S. government. President Donald Trump has rejected the notion that President Putin targeted and attempted to influence the 2016 election; however, the intelligence community (including CIA, FBI, NSA, and ODNI) released an unclassified assessment of Russian influence and direction.

> We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.[20]

---

[19] Snyder, Timothy. *The Road to Unfreedom: Russia, Europe, America*. First ed., 2018.

[20] Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." *Assessing Russian Activities and Intentions in Recent US Elections*, ODNI, 6 Jan. 2017. www.dni.gov/files/documents/ICA_2017_01.pdf.

These parts of the Intelligence Community (IC) further assess that the campaign, directed by Putin, was hybrid in nature. This campaign utilized covert cyber intelligence operations as well as "overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls'." The IC has also stated that Russia has had a long-time desire to undermine the U.S.-led liberal democratic order.[21]

Undermining U.S. democracy in a globalized cyberage environment has become much less difficult. The proliferation of online social media has become a perfect medium for influencing operations and information warfare. The ease of penetration by adversaries to effectively disseminate any desired information to a large portion of the population is troubling. Specifically, the use of Facebook, Twitter, Instagram, and Google were used as platforms to expose American voters to Russian propaganda. The Internet Research Agency (IRA), a Russian cyberwar center, attempted to manipulate opinions of Europeans and Americans about the Ukrainian conflict as well as the 2016 presidential election. The IRA had about 470 Facebook sites claiming to be American political organizations and six of them had 340 million shares of content each. Types of manipulation included Anti-Muslim ads, to people in Michigan and Wisconsin, as well as falsely declaring that one could vote by text message.[22] The FBI has a role to play in this arena; it has already removed many Facebook accounts, because of "coordinated

[21] Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." *Assessing Russian Activities and Intentions in Recent US Elections*, ODNI, 6 Jan. 2017. www.dni.gov/files/documents/ICA_2017_01.pdf.

[22] Snyder, Timothy. *The Road to Unfreedom: Russia, Europe, America*. First ed., 2018.

inauthentic behavior".[23] The FBI needs to continue this work to find and intervene when IRA and other Russian government associated accounts are found. The private sector also has an important role to play in combating this threat—the government and private sector working together to address this threat is essential and is considered in greater detail in my recommendations.

Leading up to the election, the FBI discovered Russian cyber-infiltration of the Democratic National Committee (DNC). Additionally, it became clear that Russia was able to get into White House and Department of State systems, gaining access to classified emails. During these attacks, Moscow was not terribly concerned with the U.S. knowing it was behind the attacks and even fought to stay in the systems even after being discovered.[24] After stealing information, Russia has utilized various tools to launder and disseminate it publicly, including to WikiLeaks.

As stated in the 2017 National Security Strategy, "Rival actors use propaganda and other means to try to discredit democracy. They advance anti-Western views and spread false information to create divisions among ourselves, our allies, and our partners."[25] During the Ukrainian conflict and the 2016 election, we have seen more direct actions, an increase in the level of activity, and a widening scope of effort compared to previous operations. It was even determined that "Russian intelligence

---

[23] Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age / David E. Sanger.* First ed., 2018.

[24] Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age / David E. Sanger.* First ed., 2018.

[25] United States, The White House. (2017, December). *National Security Strategy of the United States of America*. Retrieved April 16, 2019, from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

obtained and maintained access to elements of multiple US state or local electoral boards".[26] In this case, DHS assessed the systems compromised were not involved in vote tallying.[27] It is important to note the potential impact to the legitimacy and confidence in the electoral process. This was an attack on democracy; even without direct access to vote tallying or the ability to directly alter votes, it threatens American confidence in the system which is essential for peaceful transfer of power—which is a clear threat to U.S. national security.

The Conflict in Ukraine

In the years leading up to the conflict with Russia, Ukraine flirted with two mutually exclusive options: joining either the European Union or the Eurasian Union (its Russian-led counterpart in the East). Both of these regional systems of integration would benefit from Ukraine joining them in both political and economic terms. Unfortunately for Russia, despite attempts to entice Ukraine with cheap financing and energy discounts, Ukraine seemed to keep favoring the West. Most, but not all, Ukrainian citizens have a strong desire to align with the West—as evidenced by the Ukrainian Revolution in February 2014. This Revolution resulted in the removal of Ukrainian President

[26] Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." *Assessing Russian Activities and Intentions in Recent US Elections*, ODNI, 6 Jan. 2017. www.dni.gov/files/documents/ICA_2017_01.

[27] Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections." *Assessing Russian Activities and Intentions in Recent US Elections*, ODNI, 6 Jan. 2017. www.dni.gov/files/documents/ICA_2017_01.pdf.

Yanukovych for, amongst other actions, his last-minute signing of a treaty and loan agreement with Russia—instead of the association agreement with the European Union.[28]

Putin's attempts at politically achieving his goal of keeping Ukraine in the Eastern sphere of influence failed and Ukraine's trajectory turned Westward. After accepting that fact, his next move was to mitigate the negative impact it would have on Russia and demonstrate the consequences to Ukraine and other western sliding countries. In 2014, Russia occupied and annexed Crimea and subsequently began sending its troops across the border into Ukraine. This use of force was reliant on confusion and information operations. "Little green men" who were dressed in Russian uniforms without insignias and armed with modern Russian weaponry were utilized. Russia officially made remarks stating that they were Crimean self-defense forces and not Russian troops. In response to people claiming that these little green men were actually Russian troops without insignias, President Putin responded by stating: "Take a look at the post-Soviet states. There are many uniforms there that are similar. You can go to a store and buy any kind of uniform."[29] This effectively caused confusion, but U.S. officials concluded that Russian troops had crossed into Ukraine.[30] This made a common understanding of what was actually happening very difficult and domestic and international responses were effectively delayed by the Russian tactics. The strategy successfully, at least initially,

---

[28]Nadia Diuk. Euromaidan: Ukraine's Self-Organizing Revolution. April 2014.

[29] Schreck, C. (2019, February 26). From 'Not Us' To 'Why Hide It?': How Russia Denied Its Crimea Invasion, Then Admitted It. Retrieved December 17, 2019, from https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html.

[30] Butenko, V., Smith-Spark, L., & Magnay, D. (2014, August 29). U.S. official says 1,000 Russian troops enter Ukraine. Retrieved December 17, 2019, from https://www.cnn.com/2014/08/28/world/europe/ukraine-crisis/index.html.

blurred lines and caused a questioning of who the actors were and what exactly was going on—and ultimately concluded with a successful annexation of Crimea by the Russians.

Ukraine's strategic importance is not limited to the economic and political realms. As stated by Robert Donaldson and Joseph Nogee, the proposed expansion of NATO to include Ukraine in the late 2000s seriously angered Putin, who believe that "Ukrainian membership would be … catastrophic for Russia because of the historical ties between the two Slavic states, the large Russian population in eastern Ukraine, and the location of Russia's Black Sea Fleet in Sevastopol in the Crimea."[31] Crimea's geographic location makes it an extremely important strategic asset for Russia. The port city of Sevastopol is especially important for its Navy, because it is where Russia's all-important Black Sea Fleet is based. After the Soviet Union dissolved, Ukraine had been leasing the base to Russia. This base has been critical for Russian power projection in the region. The fleet enabled blockading during the war with Georgia and provides naval access to the Middle East. More recently, the Syrian civil war and Putin's support of the Assad regime made the port even more critical. Sevastopol can be, and allegedly has been, a critical supply route from Russia to Syria.[32] Currently, Crimea is claimed by both Russia and Ukraine. Additionally, despite the Minsk II agreement to a ceasefire, the conflict in eastern Ukraine continues. Meanwhile, The Organization for Security and Cooperation in

[31] *Donaldson, Robert and Nogee, Joseph.* The Foreign Policy of Russia. Changing Systems, Enduring Interests. N.Y.: M.E. Sharpe, 2009. – Russia and the Near Abroad. P. 339-376.

[32] Yuhas, Alan, and Raya Jalabi. "Ukraine Crisis: Why Russia Sees Crimea as Its Naval Stronghold." *The Guardian*. 7 Mar. 2014.

Europe has set up a Special Monitoring Mission in Ukraine to "observe and report in an impartial and objective way on the situation in Ukraine; and to facilitate dialogue among all parties to the crisis."[33]

Proxy Sanctuary

General Philip M. Breedlove, who was the Supreme Allied Commander Europe of NATO Allied Command Operations from May 2013 until May 2016, has stated:

> Competitors have operationalized hybrid strategies and brought together multiple lines of effort to achieve goals that can threaten our security. … Russian military actions in the Ukraine crisis reflect a sophisticated, complex, multi-variant approach to the use of force to achieve decisive political objectives. Russian strategists and planners have taken the classic elements of Soviet and Russian military thinking, combined them with 21st century tools, tactics, and capabilities, and created new models for military action that are adapted to Russia's strategic situation.[34]

Modern Russian campaigns, including inside Ukraine, have included the use of proxy forces to achieve Russian goals—also called "Proxy Sanctuary".[35] Additionally, of great importance in cyberage campaigns has been the targeting and exploitation of the adversary's population through advanced information and influence operations. Russia has been able to accomplish significant effects and impacts on its adversaries through the dedication of resources and effort to leverage the modern information environment. This

---

[33] "OSCE Special Monitoring Mission to Ukraine." *OSCE*, www.osce.org/special-monitoring-mission-to-ukraine.

[34] Larsen, Jeffrey Arthur, et al. "NATO's Response to Hybrid Threats." *NATO's Response to Hybrid Threats*, NATO Defense College, 2015.

[35] Karber, Phillip. *Russia's 'New Generation Warfare'*. National Geospatial Intelligence Agency, 4 June 2015.

has been a target on the people/societal part of Clausewitz's trinity. The election interference has also started to trickle over into threatening governance structures through direct attacks compromising security which could impact the confidence in the electoral system.

NORAD/USNORTHCOM commander General O'Shaugnessy has described Russia's actions as "exploiting gaps between the traditional understanding of 'peace' and 'war'", with the goal of advancing Moscow's interests by aggressively encroaching on the sovereignty of its neighbors including in Ukraine. He also recognizes the difficulty in figuring out how to respond in ways that help to solve the problems and deter this type of behavior in the future.[36]

In the 2018 National Cyber Strategy, signed by President Trump, it is made clear that "America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace".[37] It is clear that the IC is committed to the recognition and defense of the nation's cyber security regardless of where the threats originate. The IC publicly claims with high confidence that "Russia, Iran, and North Korea have conducted reckless cyber-attacks that harmed American and international businesses".[38]

As an attempt to deter Russian interference in the 2020 election, U.S. Cyber Command publicly threatened to release personal information of "senior members of

---

[36] O'Shaughnessy, Terrence J, et al. "Strategic Shaping: Expanding the Competitive Space." *Joint Forces Quarterly 90*, 3 July 2018.

[37] United States, Office of the President. "National Cyber Strategy of the United States of America." *National Cyber Strategy of the United States of America*, The White House, 2018.

[38] United States, Office of the President. "National Cyber Strategy of the United States of America." *National Cyber Strategy of the United States of America*, The White House, 2018.

Russia's government as well as Russian oligarchs, stopping short of targeting Vladimir Putin himself", if Russian interference operations were attempted.[39] This type of warning and threat could help to deter these type of actions. Stopping short of threatening the release of President Putin's information could also help to contain some further Russian escalation—and holding information on Putin in reserve as leverage that the U.S. could use at a different time could prove valuable. In addition, economic sanctions, political pressure, and cyber counterattacks should continue to be considered and utilized as necessary in reaction to actions taken by Russia against the United States. These measures need to be supported by both the executive and legislative branches in order to achieve meaningful effects. The use and coordination of multiple levels and departments within one government towards the same goal is referred to as a whole-of-government approach. It is essential to use this approach in order for the government to be more efficient, effective, and decrease redundancies. In many cases, this approach can be more likely to accomplish the policy objectives.

Defending against threats in the cyber domain require a coordinated and unified effort, which is why it is vital that the entire executive branch commit to public recognition of Russian attacks and the defense of the nation against this threat. It is critical for national security to protect the democratic system and retain the confidence in electoral processes. As such, one way to protect the process and retain citizen confidence is a paper/mail-in ballot system similar to that utilized by Colorado be implemented

[39] Evans, Z. (2019, December 26). U.S. Preparing to Respond to 2020 Russian Election Interference by Releasing Kremlin Officials' Personal Info. Retrieved April 23, 2020, from https://www.nationalreview.com/news/u-s-preparing-to-respond-to-2020-russian-election-interference-by-releasing-kremlin-officials-personal-info/

nationwide. This would severely cripple the attempts of malevolent actors to be able to interfere with the accuracy and legitimacy of an American's vote. Implementing this recommendation faces formidable political obstacles, but if achieved would provide much greater security and confidence. The For the People Act of 2019 has a subsection named the Voter Confidence and Increased Accessibility Act of 2019. It was passed in the U.S. House of Representatives on March 8th, 2019 but has not made it through the U.S. Senate. Section 1502 of the Act addresses the paper ballot issue:

> The voting system shall require the use of an individual, durable, voter-verified paper ballot of the voter's vote that shall be marked and made available for inspection and verification by the voter before the voter's vote is cast and counted, and which shall be counted by hand or read by an optical character recognition device or other counting device.[40]

Passage of the Act would represent a major step toward securing U.S. elections against what are likely to be more sophisticated attacks than occurred in 2016.

In addition, in order to help defend against foreign influencing operations and strengthen national and homeland security, the United States should implement what I would propose to call the Responsible Patriot Liaison (RPL) program. This program would work similarly to the model used in Terrorism/Threat Liaison Programs, such as seen between the Colorado Information Analysis Center (CIAC) and its public and private sector partners—which are called Threat Liaison Officers. The RPL program would forge these partnerships to defend against this and other threats. There will continue to be a fierce debate on privacy vs. national security; however, foreign influence

[40] Sarbanes, J. P. (2019, March 14). Text - H.R.1 - 116th Congress (2019-2020): For the People Act of 2019. Retrieved April 23, 2020, from https://www.congress.gov/bill/116th-congress/house-bill/1/text#

campaigns have targeted democracy and attempted to erode the foundations on which it stands. It is essential for private companies to take more responsibility in protecting the U.S. and its citizens from the type of Russian operations seen during U.S. elections. Responsible Patriot Liaisons (RPLs) would be employees from companies that have been utilized for these types of attacks such as Facebook, Twitter, Instagram, and Google. The RPL volunteer would be cleared for information related to these threats and, when necessary, will be given assistance by the government to combat these threats. Additionally, the RPL would be the contact for the government if assistance from the company is necessary.

Google, Twitter, and Facebook have voluntarily agreed to help with tackling disinformation on their platforms in the European Union and the European Commission produced a report in June 2019 regarding the relationship:

> Disinformation is a rapidly changing threat. The tactics used by internal and external actors, in particular linked to Russian sources, are evolving as quickly as the measures adopted by states and online platforms … Online platforms have a particular responsibility in tackling disinformation. Today the Commission also publishes the latest monthly reports by Google, Twitter and Facebook under the self-regulatory Code of Practice on Disinformation. The May reports confirm the trend of previous Commission assessments. Since January, all platforms have made progress with regard to the transparency of political advertising and public disclosure of such ads in libraries that provide useful tools for the analysis of ad spending by political actors across the EU. Facebook has taken steps to ensure the transparency of issue-based advertising, while Google and Twitter need to catch up in this regard.[41]

[41] A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council. (2019, June 14). Retrieved April 23, 2020, from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2914

A similar type of voluntary agreement could also prove useful between the United States and various private sector companies with the designated RPL being the contact for related issues.

To counter the effectiveness and impact of Russian information and psychological operations on the U.S. military, the United States should implement an awareness training program for deploying units. This program would expose these units to specific types of adversarial tactics and reduce psychological impact in the field. Using electronic warfare assets to try to block these operations would also be advised. The employment of cyber defenders or self-defense hacking units will deter and decrease the effectiveness of such operations against U.S. and allied forces.

It is clear that operations security (OPSEC) has been threatened by the use of personal technology by soldiers in deployed environments. The use of personal fitness apps with GPS tracking has created publicly available information that can be used to find locations of military bases and regular routes taken by solders. As a quick fix to the problem, On August 6, 2018, the Pentagon stated that "Defense Department personnel are prohibited from using geolocation features and functionality on government and nongovernment-issued devices, applications and services while in locations designated as operational areas".[42] Issues like these will continue to occur as new technology becomes available. New technologies will continue to be developed and utilized at a rate faster than policy analysis, development, and implementation can occur. To recognize and adapt to new technologies as quickly as possible, the U.S. should task a small analytical

[42] Garamone, Jim. "New Policy Prohibits GPS Tracking in Deployed Settings." *U.S. DEPARTMENT OF DEFENSE*, 6 Aug. 2018.

unit within each operational governmental organization with proactive analysis of its own OPSEC in the realm of new technologies and applications. This unit would also make recommendations on the policies regarding use of these technologies. The U.S. government must not be reactive in the realm of OPSEC. Implementation of policies restricting the type of GPS devices allowed on base should not occur after significant damage to national security has occurred. Securing national security must be proactive; focusing a group of analysts on emerging technological threats will help increase the awareness of potential future technological threats.

Sino-U.S. Relations and Managing China's Rise

"We are facing increased global disorder, characterized by decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security…China is a strategic competitor using predatory economics to intimidate its neighbors while militarizing features in the South China Sea."[43] —2018 National Defense Strategy

China has been growing at a rapid rate economically, militarily, and technologically. With the increase in power and influence, we have witnessed China increasingly acting as a revisionist power. The Chinese government has made clear that it intends to change the status quo and gain a a stronger and more influential position in its region and globally. As the strongest global power and greatest benefactor of the status quo, the United States sees China as a major threat to U.S. interests. China recognizes the U.S. as the greatest obstacle to revising the world order and accomplishing its major policy goals. Various Chinese actions have stoked major concern in the United States. For example, China has been aggressively targeting the U.S. and others through various means including hacking, cyber warfare, espionage, and attempts to alter territorial boundaries in the South China Sea. These activities are enduring threats to the U.S. and its partners.

[43] Mattis, J. (2018, January 19). Summary of the National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Every country, to include the United States, has limited resources. In an attempt to allocate limited resources as effectively as possible, for the defense of the country and promotion of national interests, assessment and prioritization of threats and challenges is essential. To designate something as a "threat" requires an actor to have both capability and intent. China is a threat to the United States in some specific areas (particularly in the cyber domain) and is a threat to U.S. interests; however, China does not currently pose an existential threat to the United States homeland or to the destruction of the international order.

At this point, there is no evidence that China intends to engage in armed conflict with any major power or completely overthrow the international order. It is not in the best interest of the government to attempt either of these. Beijing clearly seeks to continue growing its economy and gain greater influence in current systems. China wants a greater share of influence and decision-making ability, which could take place in current systems and organizations. Beijing has also launched major new initiatives in order to extend its influence, most notably the Belt and Road Initiative (BRI) and the Asian Infrastructure Investment Bank (AIIB).

How the U.S. reacts to the growth of the Chinese economy and increasing political influence will greatly impact the future of the international order. The geopolitical environment in the Indo-Pacific has been changing and will continue to change with the growth of China. As much as possible, the United States must adapt to these circumstances and utilize a whole-of-government approach to influence and shape these inevitable changes to protect U.S. interests as much as possible. Attempting to contain China, as it once contained the Soviet Union will not work; China's economy is

more diversified and, due largely because of the size of its population and impressive economic growth, China is emerging as a peer competitor both economically and militarily. Moreover, the ruling Communist Party has maintained internal cohesion, in large part through repression and the extensive use of surveillance technology. As such, the United States must recognize that a policy that tries forcibly to contain China will increase adversarial tension and, while it may slow China down, will likely fail in the long run. China's strategy is long-term and U.S. policy must also focus on longer-term interests. To address Chinese strategic competition, and protect long-term U.S. interests, the U.S. should adopt a policy to manage China's rise. If the United States is not involved heavily in the region, the vital U.S. interest of advancing American influence (Trump's fourth pillar) with not be furthered.

Managing China's Rise

The first requirement of creating a sound strategy and subsequent policy is a proper assessment of the strategic facts on the ground and context of the heavily globalized strategic environment. The basic premise of this strategy is the realization that China will continue to rise, even if Western nations try to forcibly contain it. Consequently, a policy of strong containment would, at most, provide short-term benefits and would likely sacrifice longer-term interests. The primary long-term goal of managing China's rise is a minimally altered U.S. led international order with a China that acts as a responsible, invested shareholder in the current order. It is counterproductive and a waste of limited resources to try to contain China and struggle with Beijing at every turn—and

this policy will ultimately fail anyway. Instead, the United States should pick its battles wisely, prioritize the most important long-term goals, and provide incentives for Beijing to be more invested in the current world order as it continues to grow economically and gain more influence. This will require some short-term sacrifices, which I will propose in later sections, but ultimately will promote the continuation of a U.S. led international order that has greater adaptability. In today's rapidly evolving global environment, adaptability is absolutely critical to the long-term success of an international order. A static system that continually fights change at every turn is a system that is destined for failure, but a system that adapts and effectively manages change may thrive.

Chinese Threats and Challenges

Graham Allison argues in *The Atlantic* that "the defining question about global order for this generation is whether China and the United States can escape Thucydides's Trap."[44] After his team at Harvard analyzed the historical record of rising revisionist powers, he points out that twelve of sixteen cases over the past 500 years resulted in war. Additionally, he argues that "based on current trajectory, war between the United States and China in the decades ahead is not just possible, but much more likely than recognized".[45] While great power transitions are incontestably dangerous, Allison fails to emphasize the extent to which nuclear weapons have substantially raised the risk and cost

[44] Allison, Graham. "The Thucydides Trap: Are the U.S. and China Headed for War?" *The Atlantic*, Atlantic Media Company, 24 Sept. 2015

[45] Allison, Graham. "The Thucydides Trap: Are the U.S. and China Headed for War?" *The Atlantic*, Atlantic Media Company, 24 Sept. 2015,

of war between great powers. While there will continue to be significant competition and confrontation between the U.S. and China, it is difficult to imagine that both China and the U.S. would be willing to risk total war. They have a strong incentive therefore to seek a *stable balance*—even if that requires substantial compromise. The current relationship with China is adversarial for many reasons politically, economically, and militarily—which all make progress difficult. However, making efforts now to create a more positive and less adversarial Sino-American relationship may increase China's willingness to assimilate into an international order with fewer revisions than are currently being sought.

Pessimism about China's intentions is largely based on the assumption of indefinite rule by an authoritarian regime bent on expansionism. Some scholars point out another possibility, in which the economic liberalization required for continued growth leads to political reform. Hahm Chaibong, President of the Asan Institute for Policy Studies, in Seoul, South Korea, believes that the growth may actually lead to the transformation of the authoritarian regime. In *China's Future is South Korea's Present* he wrote:

> There are two possible paths for China going forward: political liberalization, which would enable continued economic success, or authoritarian retrenchment, which would slowly but surely undermine China's economic growth. The lesson of South Korea is that when it comes to sustaining economic growth, political liberalization is not a matter of choice.[46]

Chaibong argues that economic liberalization generates pressures that even authoritarian leaders cannot fully repress. If this assessment is correct, it would be possible that China

[46] Chaibong, Hahm. "China's Future Is South Korea's Present." *Foreign Affairs*, vol. 97, no. 5, Sept. 2018.

is on a path towards political liberalization similar to what was seen in South Korea—as democratization and rapid economic growth turned it into a model for the appeal of a liberal internationalist world order. Taking a harder line on China may impede that prospect and be counterproductive.

The recent protests and riots in Hong Kong, stemming from China's desire for greater political control in the region, point to the possibility that China is starting to see significant effects from economic liberalization. Even with broad censorship across the internet, people still communicate and act through other means. The protests in Hong Kong against increased mainland government control, seem to provide added support for Chaibong's argument, as President Xi has apparently concluded that crushing Hong Kong's human rights demonstrators is not worth the prospective economic and political costs. That hesitation could even lead to an increase in pressure within China for political liberalization.

Balancing the need for close diplomatic relations with the need to deter Chinese actions counter to U.S. interests is a daunting task, and one can hardly exclude situations that make these two goals mutually exclusive. One area that has been degrading the Sino-U.S. relationship is the cyber domain. Even though attribution in this environment can be extremely difficult, there have been attacks that the U.S. believes with high confidence have been sponsored by the Chinese government. This has made fostering this relationship increasingly difficult, but there are actions that can and must be taken to mitigate some of the damage.

Cybercrimes, Hacking, and Espionage

David Sanger, in *The Perfect Weapon*, describes the relationship between China and the U.S. as a "new cold war between the world's two largest economies." Sanger argues that China's interests extend beyond territorial claims, as it seeks to achieve "the keys to reemerging as a global power … [through] artificial intelligence, space technology, communications, and the crunching of big data." That goal, he notes, requires China to outmaneuver the United States.[47]

Cyber espionage, hacking, and intellectual property theft have become major points of tension between the U.S. and China as well as other countries. As stated in the 2016 U.S. National Security Strategy: "Every year, competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars. Stealing proprietary technology and early-stage ideas allows competitors to unfairly tap into the innovation of free societies".[48]

In Operation Aurora, conducted in 2009, Chinese hackers breached Google's security and searched for source code from Google's search engine. They wanted to recreate Google's successes and create a more state favorable internet search engine within China. This type of cyber activity hurts the economies of countries, but generally has minimal impact on international security. However, as part of operation Aurora, the

[47] Sanger, D. E. (2019). *The Perfect Weapon: War, sabotage, and fear in the cyber age*. New York: Broadway Books.

[48] United States, The White House. (2017, December). *National Security Strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Chinese were able to get ahold of court documents from the United States Foreign Intelligence Surveillance Court and other judges around the country. This gave a serious advantage to China's clandestine intelligence establishment. The ability of Chinese intelligence to know if its spies are compromised and under investigation, before they have actually been charged with a crime, is extremely advantageous.[49] This has serious potential to undermine the FBI's counter-intelligence operations and significantly weaken national security.

The U.S. Office of Personnel Management (OPM) hacks were another case with large potential consequence to U.S national security. In the summer of 2014, the SF-86 forms for 21.5 million people were copied from the OPM's database. By the end of the year, 4.2 million personnel files were stolen—which included social security numbers and other sensitive information. In addition, 5.6 million fingerprints also ended up stolen. The damage to the U.S. national security apparatus was clear. With this information, it would be much easier to track down spies, hack into people's accounts, find cleared federal employees, determine best or most vulnerable targets for blackmail and bribery, and utilize or share this information in many other damaging ways.[50]

Another complicating factor is that even though these capabilities and types of attacks seem to be highly detrimental, many countries that have advanced cyber prowess are hesitant to give capabilities up or pursue meaningful agreements to stop or limit

[49] Sanger, D. E. (2019). *The Perfect Weapon: War, sabotage, and fear in the cyber age*. New York: Broadway Books.

[50] Sanger, D. E. (2019). *The Perfect Weapon: War, sabotage, and fear in the cyber age*. New York: Broadway Books.

usage. Some types of cyber tactics are also not universally considered extremely dangerous or a major slippery slope. In regard to the Chinese hacks on the U.S., the former Director of National Intelligence, James Clapper actually respected Chinese cyber-espionage and understood why they decided to perpetrate these operations, saying: "You have to kind of salute the Chinese for what they did." Additionally, Clapper wanted to make it known that this was not only one-sided and that "if we had the opportunity to do the same thing, we'd probably do it".[51]

These types of attacks can also interfere with diplomacy and bilateral or multi-lateral agreements—which can have international security complications. Constant cyber-attacks create a continual sense of conflict between the countries which foments an adversarial mentality. This is true not only for the leaders, but also extends to citizens of the countries attacked as well. Attacks can also affect a state's sovereignty and human security. For example, cyber-attacks on a state's democratic electoral process clearly interferes with state sovereignty and governance, while sabotaging a power grid can cause death and other serious societal consequences.

> We know hackers steal people's identities and infiltrate private emails, … We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic-control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy[52] – President Obama

[51] Sanger, D. E. (2019). *The Perfect Weapon: War, sabotage, and fear in the cyber age*. New York: Broadway Books.

[52] Obama, B. (2013, February). *The 2013 State of the Union Address*. Washington D.C.

Capability is growing and attacks that actually cause physical damage or put people in danger have already occurred.

Internationally, there is currently a major gray area regarding cyber weapons and tactics. There is frequent, if not constant, conflict occurring in the cyber realm that has mostly stayed below the threshold of escalating to physical violence between states—the most public exception to this being the Israeli airstrike on a what its military said was "HamasCyberHQ". In this instance, the military stated that they "thwarted an attempted Hamas cyber offensive against Israeli targets" and "targeted a building where the Hamas cyber operatives work."[53] Managing escalation is essential, but the location of the exact line in the sand (or code) remains in question. The limits on escalation are also clearly dependent on the adversary and their respective escalatory capabilities.

In the past, there has been reported Chinese hacking that targeted energy infrastructure and oil.[54] How leaders interpret such attacks has profound security implications. Attacks that could impact or threaten human security or critical national infrastructure could be designated as acts of war and could potentially start a major kinetic conflict. Attacks that have negative impacts on national security would be more likely to elicit a response, but at what point a victim is willing to escalate depends on a vast number of factors. It also would vary from country to country and different leaders would likely have different thresholds.

---

[53] Doffman, Z. (2019, May 6). Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First. https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#53434307afb5

[54] Sanger, D. E. (2019). *The Perfect Weapon: War, sabotage, and fear in the cyber age*. New York: Broadway Books.

The U.S. itself is suspected to be among the many actors that have used cyber capabilities to significantly damage an adversary's national assets—one example being the Stuxnet computer worm attack on Iran. Iranian centrifuges used to refine nuclear material were suspected to be damaged by a U.S./Israeli cyber-attack, which significantly set back the country's nuclear program.[55] Some of these attacks can potentially be executed by sophisticated non-state actors as well—which further complicates the creation of clear policies or international laws regarding cyber-attacks. Additionally, the difficulty in correctly attributing cyber activities to a specific actor adds a significant component of complexity and difficulty in the policy and decision-making process.

One response tactic to the use of cyber weapons/attacks is to react immediately both physically and decisively, which Israel utilized in May of 2019.

> The Israel Defense Forces (IDF) … launched a physical attack on Hamas in immediate response to an alleged cyber-assault. The IDF hit a building in the Gaza Strip with an airstrike after claiming the site had been used by Hamas cyber operatives to attack Israel's cyber space.[56]

If attribution can be made with high-confidence, this type of response may be effective against terrorists or other non-state actors who are in current warzones and are targeting critical infrastructure—or other assets that are critical to national security. In such cases, maximizing deterrence would involve publicized threats linked to prospective cyber-targets. If executed successfully, this response could stop active attacks, destroy critical

---

[55] Groll, E. (2016, October 17). 'Obama's General' Pleads Guilty to Leaking Stuxnet Operation. Retrieved April 1, 2020, from https://foreignpolicy.com/2016/10/17/obamas-general-pleads-guilty-to-leaking-stuxnet-operation/

[56] O'Flaherty, K. (2019, May 08). Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First. https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/#3251c7b9f895

personnel and equipment required to conduct attacks, and also serve as a deterrent for future attacks from some other actors. However, this is clearly not an appropriate response to non-state actors perpetrating cyber-attacks from within another sovereign territory outside of a warzone. Ideally, the other state would be able and willing to assist in finding and stopping the threat; however, it is much more difficult in cases where the threat is originating from an adversarial nation that might either be supporting the actors or have no incentive to stop them.

It is difficult to react to cyber threats from within other adversarial nations' territory except for increasing cybersecurity defenses—especially if the U.S. itself wants to retain the right to use this capability itself whenever it deems necessary. In terms of cyber-espionage, exploiting weaknesses is the typical *modus operandi* and will certainly continue to occur. However, agreements and accords can help to make progress in other areas. Even if accords are not comprehensive and fall short of effectively prohibiting activities in this domain, it will still create a dialogue and understanding between the states regarding what is known and allowed in the relationship—which is important for a healthy and cooperative relationship. According to Sanger, after Obama announced an accord that curbed some of the cyber means of intellectual property theft, there was actually a "marked drop-off in that kind of hacking by the Chinese".[57] Therefore, it seems some progress can be made, even though cyber-arms control meets heavy resistance by states that have already developed advanced capabilities.

[57] Sanger, D. E. (2019). *The Perfect Weapon: War, sabotage, and fear in the cyber age*. New York: Broadway Books.

It is time the U.S. responds to address the deepening danger of cyber-attacks originating from within sovereign states by initiating an ongoing international dialogue aimed at establishing norms and guidelines in order to decrease the risks of miscalculation. Additionally, the U.S. must increase cyber defenses through coordination and sharing of information with its allies. Working with other states by communicating when and how attacks occur can increase the ability to defend against these attacks. Having technical knowledge of how the perpetrators are attacking can help prepare and provide resilience—much like getting a vaccination ahead of time to prepare a body's immune system by building up its defenses to fight off specific types of biologic threats. The U.N. Institute for Disarmament and Research has noted the glaring absence of such and institutional effort:

> Cyber specialists within regional organizations have themselves identified the need to have an opportunity to meet with their peers from other regions in order to explore opportunities for inter-organizational cooperation, exchange of information and lessons, and potential informal (or more formal) mechanisms for collaboration. While they often do so on the margins of other meetings, thus far there lacks a structured opportunity in a neutral space for regional organization representatives to discuss specific challenges, exchange ideas and share resources. No one organization is "mandated" to convene the others and attempts to do so thus far have been stymied by politicization by some members.[58]

Should such an international dialogue be created, it should include creation of an international database which catalogs Information and Communication's Technologies (ICT) threats and categorizes them by type of attack and (as much as possible) by location. The information would come from public and private sector organizations

[58] The Role of Regional Organizations in Strengthening Cybersecurity and Stability. (2019, January 24). Retrieved April 1, 2020, from https://www.unidir.org/publication/role-regional-organizations-strengthening-cybersecurity-and-stability

worldwide after an attack has occurred. This database would be able to be accessed by anyone, but the information on the type of vulnerability exploited would be provided by the victim of the attack only to trusted partners. According to U.N. General Assembly Resolution 73/27 (A/RES/73/27) Section 1.11:

> States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.[59]

Thus, this database should be managed by the United Nations, possibly through the Open Ended Working Group—which is focusing on developments in the field of information and telecommunications in the context of international security. Knowledge of the type of vulnerabilities that have been found and exploited can enable members to patch their software and reduce/counter these vulnerabilities.

While states are likely to share some information formally and informally with certain allies and partners, this international database administered by the U.N. would provide data that can be utilized for various assessments. It can help create a better threat picture and shed some light on a domain that is very esoteric. Illuminating the types of threats and attacks, as well as where they originate, may help to determine the degree to which certain state and non-state actors are involved and provides the foundation for greater cooperation and resilience. It can also lead to legitimate calls to action against cyber-aggression from Russia, China, Iran, North Korea, and other state and non-state actors.

---

[59] A/RES/73/27 Developments in the field of information and telecommunications in the context of international security. (2018, December 11). Retrieved April 1, 2020, from https://undocs.org/en/A/RES/73/27

South China Sea

The South China Sea is a major economic corridor: $3.37 trillion worth of trade passed through this sea in 2016 alone. Additionally, 40% of global liquefied natural gas trade transited through in 2017. Since 2013, China has created 3,200 acres of new land in disputed waters in the Spratly Islands [see appendix]. The South China Sea is also rich in mineral resources. It is estimated to hold 11 billion barrels of oil and 190 trillion cubic feet of natural gas.[60] The building of artificial islands, in an attempt to harden its territorial claims and militarize the Spratly Islands, is an attempt to subvert ordinary means to resolve territorial disputes and undermine U.S. influence. According to the 2019 DNI Worldwide Threat Assessment: "China will continue increasing its maritime presence in the South China Sea and building military and dual-use infrastructure in the Spratly Islands to improve its ability to control access, project power, and undermine US influence in the area."[61] Territorial aggression in the South China Sea is one of the significant challenges posed by China to the international order. As Patrick Cronin characterizes the threat:

> Beyond Asia, the South China Sea is at the nexus of the global economy upon which all major trading nations' prosperity depends. About 90 percent of global commercial trade is seaborne, and more than a third of all that trade crosses the

[60] Territorial Disputes in the South China Sea | Global Conflict Tracker. (2019, May 31). Retrieved from https://www.cfr.org/interactive/global-conflict-tracker/conflict/territorial-disputes-south-china-sea

[61] Coats, D. R. (2019, January 29). *Worldwide Threat Assessment of the US Intelligence Community* (United States,Office of the Director of National Intelligence). https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR-SSCI.pdf

> South China Sea … where America's ability to project power in support of freedom of the seas is increasingly open to question.[62]

Cronin correctly argues that the future stability of the region and international order (especially at sea) is at stake. It is not the specific rocks, reefs, and resources that are of the biggest concern, but instead the bigger picture of the actions being taken by the growing revisionist power. In Cronin's view, the U.S. should not go a single day without sailing its vessels through the South China Sea or flying its aircraft over the islands. Doug Bandow, however, challenges that approach as provocative and counterproductive:

> For Washington to attempt to coerce the PRC over interests viewed in Beijing as important if not vital guarantees a much more confrontational relationship. China likely would respond by matching American air and naval maneuvers, accelerating military outlays, and challenging U.S. interests elsewhere. Indeed, turning today's regional dispute into a quasi-superpower confrontation would raise the stakes and make the issues harder to resolve.[63]

Bandow argues that the U.S. should withdraw from East Asia, abandon the fight for regional hegemony, and withhold security guarantees from threatened states, and take no position regarding competing territorial claims. That argument is flawed. China will continue to get stronger economically—albeit at a less rapid pace than seen in the recent past—and will have the resources and desire to continue to build its military. A U.S. departure from the region would leave a vacuum that would almost certainly be filled by China. Abandoning allies now would be a disaster politically and militarily, placing vital trade routes under Chinese control, and signaling worldwide the likelihood that the U.S.

---

[62] Cronin, Patrick M. "America Must Take a Stand in the South China Sea." *The National Interest*, The Center for the National Interest, 2016, nationalinterest.org/print/feature/america-must-take-stand-the-south-china-sea-13779.

[63] Bandow, Doug. "The Ultimate Irony: Is China the 'America' of Asia." *The National Interest*, The Center for the National Interest, 25 Sept. 2016, nationalinterest.org/print/feature/the-ultimate-irony-china-the-america-asia-12976.

will retreat when a revisionist power challenges the status quo. However, Bandow does raise a persuasive challenge to Cronin's faith in a more robust strategy of deterrence. China is becoming stronger and will perceive certain interests, including in the South China Sea, as vital to its national security—even if defending those interests entails high cost and risk.

Cronin and Bandow both make important points, but neither complete withdrawal nor attempting aggressive and robust military deterrence are viable solutions. Using only military strength and maneuvers to coerce and antagonize one another may preserve status quo in the short-term but involves an unavoidable risk of miscalculation, while deepening the cold war atmosphere characterizing Sino-U.S. relations. To formulate a more effective and longer-term South China Sea policy, significant diplomatic efforts must be undertaken by both sides. This will include the willingness to compromise and find solutions that both sides ultimately can put to paper and agree upon.

To achieve this goal, the U.S. and key partners will likely have to nudge Chinese decisionmakers towards an acceptable solution using a diverse set of capabilities and resources. The situation in the SCS must be handled using a more efficient, highly coordinated U.S. led multinational effort, which must take a more robust whole-of-government approach carefully utilizing several different diverse elements of national power. The Department of State would lead this effort but would involve many other parts of the government including the Department of Defense and other interagency partners. This approach must include a strong long-term strategic diplomacy, a carefully planned strategic messaging campaign, and economic/trade agreements with allies and partners in the region. The creation of multilateral agreements with as many partners and

allies in the region will be essential to presenting a united and determined front opposing aggression in the SCS; there is strength in numbers and ultimately this will enable all parties involved to keep SCS operations more aligned with the environment in the past—although all parties must be willing to find a middle ground. This middle ground will be hard to negotiate and likely take many rounds of negotiations with the various interested parties.

A temporary understanding will likely need to entail an arrangement somewhat similar to the dispute over Taiwan. According to the U.S. Department of State:

> The United States and Taiwan enjoy a robust unofficial relationship. The 1979 U.S.-P.R.C. Joint Communique switched diplomatic recognition from Taipei to Beijing. In the Joint Communique, the United States recognized the Government of the People's Republic of China as the sole legal government of China, acknowledging the Chinese position that there is but one China and Taiwan is part of China. The Joint Communique also stated that the people of the United States will maintain cultural, commercial, and other unofficial relations with the people of Taiwan. The American Institute in Taiwan (AIT) is responsible for implementing U.S. policy toward Taiwan. The United States does not support Taiwan independence. Maintaining strong, unofficial relations with Taiwan is a major U.S. goal, in line with the U.S. desire to further peace and stability in Asia. The 1979 Taiwan Relations Act provides the legal basis for the unofficial relationship between the United States and Taiwan, and enshrines the U.S. commitment to assist Taiwan in maintaining its defensive capability. The United States insists on the peaceful resolution of cross-Strait differences, opposes unilateral changes to the status quo by either side, and encourages both sides to continue their constructive dialogue on the basis of dignity and respect.[64]

The U.S.-Taiwan relationship should continue to remain with this understanding. Although the U.S. does not support Taiwan independence, it has committed to "assist in maintaining its defensive capability" and "opposes unilateral changes to the status quo by

[64] U.S. Relations With Taiwan - United States Department of State. (2020, February 13). Retrieved May 14, 2020, from https://www.state.gov/u-s-relations-with-taiwan/

either side."[65] This wording does not officially commit the United States to defending Taiwan militarily, but only assisting in maintaining Taiwan's capability for defense. However, if China were to attempt to make "unilateral changes to the status quo", this wording does not specifically exclude the possibility that the U.S. could actually provide some sort of active military defense. If China were to perceive that the U.S. is not committed to the defense of Taiwan, then a forceful attempt at reunification may be more likely to occur. To preserve the status quo, the U.S. must continue its strong economic relations with Taiwan and its significant support for strengthening Taiwan's defensive capacity.

Politically, keeping open the option of actively engaging in the military defense of Taiwan, while not directly stating this publicly, is an appropriate policy but it must be supplemented by specific and pointed strategic messaging—including military coordination and exercises. In order to deter potential Chinese aggression, it is critical that the United States is perceived to be able and willing to defend Taiwan—regardless of whether or not the U.S. is actually willing. Until and unless all parties are willing to diplomatically negotiate towards more permanent solutions, the U.S. and its allies should continue to firmly protect the status quo—both with Taiwan and the South China Sea. The best short-term solution involves neither side officially conceding to the other. The U.S. should eventually, after returning to a policy of greater inclusion in the region, lead the charge in trying to shore up support for a more permanent diplomatic solution.

[65] U.S. Relations With Taiwan - United States Department of State. (2020, February 13). Retrieved May 14, 2020, from https://www.state.gov/u-s-relations-with-taiwan/

A potential longer-term solution in the South China Sea combines both Cronin and Bandow's arguments. The U.S. completely withdrawing from the region is not in the U.S. or its allies' best interests; however, neither is intensifying the conflict and significantly damaging U.S.-Sino relations through attempts to forcibly contain China. As China gets stronger, it naturally will fight harder for its important national interests and will build the capabilities necessary to achieve its major policy goals—as seen with the expansion of its navy. With this understanding, the U.S., its allies, and partners must strive to protect their national interests as much as possible and also, to a certain degree, allowing China to do the same. What is of greatest importance for the U.S. is protecting the vast amount of international trade that transits this sea and sustaining the international order. A negotiated agreement must include adequate protections for trade to continue as normally as possible, while also ensuring that China feels like it has adequate security along its bordering seas. Former China director of the National Security Council, James Keith, has stated: "China is fighting back against American dominance as it tries to carve out a place for itself in the region."[66] At the same time, other regional states must feel like they also have adequate space and security along their borders and in their exclusive economic zones. The Nine Dash Line (See Appendix) must be adjusted to provide a more workable and reasonable middle ground and, if all sides are open to discussing changes, a solution may still be possible.

[66] Rosenfeld, E. (2016, July 12). Sweeping ruling against China will have lasting impact globally. Retrieved April 28, 2020, from https://www.cnbc.com/2016/07/12/south-china-sea-breathtaking-ruling-against-china-to-have-lasting-impact.html

China must be willing to shrink its maritime claims—which have been deemed illegal by the Permanent Court of Arbitration in The Hauge, Netherlands with regard to international law.[67] Peter Dutton, Professor at the U.S. Naval War College and Researcher at its U.S.-Asia Law Institute reacted to this ruling: "Over time, this decision will inevitably be the basis for resolution of the disputes in the South China Sea. Equally inevitable is that a final resolution will be through negotiation between the parties. But I believe there will still be a long road ahead."[68]

Making some changes and conceding to some of China's interests for a broader regional security and economic agreement may be in the best interests of many states that are involved. Where this line is drawn must be open for discussion by all parties involved; at this point, without deep discussions between the states, it is impossible to determine exactly where that line may eventually be agreed upon. However, a workable agreement certainly requires U.S. leadership, strength, and influence at the table in order to counter-balance China and defend the other regional states' interests. Additionally, U.S. partnerships in the region must be as strong as possible in order to present a more unified multilateral front against strong Chinese assertiveness in the region. This is essential for adequately managing China's rise over the coming years.

---

[67] Rosenfeld, E. (2016, July 12). Sweeping ruling against China will have lasting impact globally. Retrieved April 28, 2020, from https://www.cnbc.com/2016/07/12/south-china-sea-breathtaking-ruling-against-china-to-have-lasting-impact.html

[68] Rosenfeld, E. (2016, July 12). Sweeping ruling against China will have lasting impact globally. Retrieved April 28, 2020, from https://www.cnbc.com/2016/07/12/south-china-sea-breathtaking-ruling-against-china-to-have-lasting-impact.html

Taking on an influential role in the Indo-Pacific is directly aligned with at least three of the Trump Administration's "four pillars" of vital national interest: American prosperity, advanced American influence, and promoting peace through strength. International relations professor at Harvard University's John F. Kennedy School of Government, Stephen Walt stated, "Trump abandoned the Trans-Pacific Partnership on his third day in office, thereby destroying a key institution that would have bound a number of Asian countries more tightly to the United States".[69] In place of the TPP, the remaining nations signed the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) with 22 items suspended that the United States wanted included.[70] The U.S. withdrawal certainly raised questions about U.S. commitment in the region. The U.S. must show greater leadership and involvement in the region or China will fill the void and U.S. interests will certainly not be protected. The U.S. should commit to reentering this agreement and negotiating favorable terms. Additionally, the U.S. needs to commit to strengthening existing partnerships and building new ones where possible. Furthermore, the U.S. should either provide enhanced alternative means of funding for Asian infrastructure or try to influence the Asian Infrastructure Development Bank by joining, as other U.S. allies have, and becoming an influential member. Greater U.S. involvement and support in the Indo-Pacific will increase influence and enable the

[69] Walt, S. M. (2017, May 3). This Isn't Realpolitik. This Is Amateur Hour. Retrieved April 26, 2020, from https://foreignpolicy.com/2017/05/03/this-isnt-realpolitik-this-is-amateur-hour/

[70] Dwyer, C. (2018, March 8). The TPP Is Dead. Long Live The Trans-Pacific Trade Deal. Retrieved April 26, 2020, from https://www.npr.org/sections/thetwo-way/2018/03/08/591549744/the-tpp-is-dead-long-live-the-trans-pacific-trade-deal

U.S. and partner nations to utilize various types of influence and pressure to achieve more favorable outcomes regarding Chinese action in the SCS and in future conflicts.

Rep. Mac Thornberry, ranking member of the U.S. House Armed Services Committee, and other congressmen believe that there is a significant need for legislation addressing U.S. commitment, action, and funding in the Indo-Pacific. In April 2020, Thornberry released a discussion draft of a potential Indo-Pacific Deterrence Initiative and stated:

> Senior officials from both parties, military commanders, and international security experts have told us for years that the Indo-Pacific must be this country's priority theater. They are absolutely correct, and it is time to put our money where our mouth is. These are not all new programs, but by pulling them together under one policy we will be better able to judge our own commitment here at home, demonstrate our resolve to our allies and partners, and deter China. We may not be able to cover all of these programs this year, but it is important that we make a start, and then use this legislation to measure our progress going forward.[71]

Legislation directing additional funding and increased U.S. involvement in the Indo-Pacific is an important step towards protecting long-term U.S. interests.

Additionally, U.S. Senate should ratify the United Nations Convention on the Law of the Sea (UNCLOS). As Congressman Hank Johnson has argued, "[t]his treaty is of paramount importance to American national security interests and our political and economic interests in Asia as well. It offers the legitimacy of the rule of law to our actions, especially in areas that are contested."[72] This would decrease U.S. hypocrisy with

[71] Thornberry Unveils Indo-Pacific Deterrence Initiative. (2020, April 16). Retrieved May 19, 2020, from https://republicans-armedservices.house.gov/news/press-releases/thornberry-unveils-indo-pacific-deterrence-initiative

[72] Johnson, H. (2016, April 18). Why the US Needs to Ratify UNCLOS. Retrieved April 28, 2020, from https://thediplomat.com/2016/04/why-the-us-needs-to-ratify-unclos/

regard to international rule of law and would provide more legitimacy to the claims of the United States, especially with regard to current challenges both in the SCS and in the Arctic—where Chinese and Russian presence are rapidly increasing. Admiral Harry Harris, former Commander of U.S. Pacific Command, also has voiced his support for ratifying UNCLOS. He believes not being a signatory negatively impacts U.S. moral standing and has an economic impact, especially in the Arctic.[73]

PLA Navy Growth and Modernization

Oriana Mastro, Assistant Professor of Security Studies at Georgetown University, has argued that China is playing the long game and semi-stealthily becoming a greater power.[74] She has adequately described the method by which the People's Republic of China (PRC) intends to achieve its major goals.

> China is building a robust, lethal force with capabilities spanning the air, maritime, space and information domains which will enable China to impose its will in the region. As it continues to grow in strength and confidence, our nation's leaders will face a China insistent on having a greater voice in global interactions, which at times may be antithetical to U.S. interests.[75] –U.S. Defense Intelligence Agency

[73] Majumdar, D. (2016, July 13). Why the United States Needs to Join UNCLOS. Retrieved April 28, 2020, from https://nationalinterest.org/blog/the-buzz/why-the-united-states-needs-join-unclos-16948

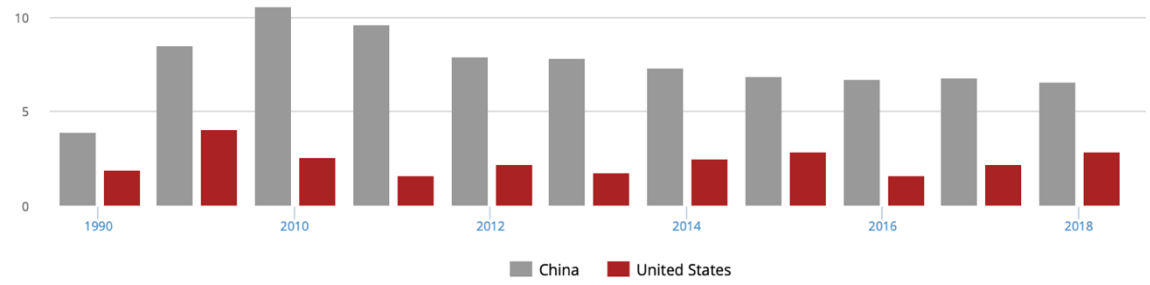
[74] Mastro, Oriana Skylar. "The Stealth Superpower." *Foreign Affairs*, Foreign Affairs Magazine, 4 Feb. 2019, www.foreignaffairs.com/articles/china/china-plan-rule-asia.

[75] United States, Defense Intelligence Agency. (2019, January 3). *China Military Power*. https://www.dia.mil/Portals/27/Documents/News/Military Power Publications/China_Military_Power_FINAL_5MB_20190103.pdf

Understanding the modernization of forces is critical when forming policy and the U.S. must be proactive in ensuring that the outcome is as favorable to U.S. interests as possible. The Rand Corporation did a comparative study of the U.S. and Chinese militaries and has determined:

> Over the past two decades, China's People's Liberation Army has transformed itself from a large but antiquated force into a capable, modern military. Although China continues to lag the United States in terms of aggregate military hardware and operational skills, it has improved its relative capabilities in many critical areas … China's improved performance could raise costs, lengthen [an Indo-Pacific] conflict, and increase risks to the United States.[76]

Economically, China's GDP growth has been significantly higher than the United States over the past few decades.[77] "The gap between the size of the two economies in terms of nominal GDP is expected to lessen by 2023; the U.S. economy is projected to grow to $24.88 trillion by 2023, followed closely by China at $19.41 trillion."[78] Below is a chart from the World Bank comparing the two nation's GDP growth as a percent:



Source: World Development Indicators

[76] Heginbotham, E., Nixon, M., Morgan, F. E., Heim, J. L., Hagen, J., Tao Li, S., … Morris, L. J. (2015). An Interactive Look at the U.S.-China Military Scorecard. Retrieved April 28, 2020, from https://www.rand.org/paf/projects/us-china

[77] World Bank. (n.d.). Data for China, United States. Retrieved April 28, 2020, from https://data.worldbank.org/?locations=CN-US

[78] Silver, C. (2020, April 17). The Top 20 Economies in the World. Retrieved April 28, 2020, from https://www.investopedia.com/insights/worlds-top-economies/

"China's double-digit economic growth has slowed recently, but it served to fund several successive defense modernization Five-Year Plans".[79] China has "built more than one hundred warships in the past decade, a build rate outstripping the mighty U.S. Navy" and is believed to be building several aircraft carriers.[80] The Peoples Liberation Army and its Naval branch (PLAN) are growing and modernizing at a rapid pace—especially with regard to its aircraft carrier program.

> Five years after commissioning its first aircraft carrier, the *Liaoning*, China launched its second carrier – the Type 001A – on April 26, 2017. Unlike its Soviet-built predecessor, the Type 001A is China's first domestically built carrier. Both carriers are similar in size and use a STOBAR (Short Take-Off But Arrested Recovery) system for the launch and recovery of aircraft. Although similar to the *Liaoning*, the Type 001A features some notable enhancements and represents an important step in China's developing aircraft carrier program.[81]

The Type 001A is suspected of being the first of three planned domestic aircraft carrier models. Enhancements are expected include an increase in airwing size, and faster cruising speed. Some key vulnerabilities include the use of a ski jump, instead of a launch system, which requires a speed of around 20 knots to launch fixed wing aircraft. It is also conventionally powered, instead of nuclear. "Beijing probably also will use the carrier to project power throughout the South China Sea and possibly into the Indian Ocean. The

---

[79] United States, Defense Intelligence Agency. (2019, January 3). *China Military Power*. https://www.dia.mil/Portals/27/Documents/News/Military Power Publications/China_Military_Power_FINAL_5MB_20190103.pdf

[80] Mizokami, Kyle. "China Could Have 4 Aircraft Carriers by 2022: Should the Navy Be Worried?" *The National Interest*, The Center for the National Interest, 12 Sept. 2018, nationalinterest.org/blog/buzz/china-could-have-4-aircraft-carriers-2022-should-navy-be-worried-31077

[81] China Power Team. "What do we know (so far) about China's second aircraft carrier?" China Power. April 22, 2017. Updated May 3, 2019. https://chinapower.csis.org/china-aircraft-carrier-type-001a/

carrier conducted initial sea trials in May 2018 and is expected to enter into service by 2019".[82]

Although the Type 001A is vastly inferior to the American Nimitz and Ford class carriers, the plans for a Type 002 and Type 003 are of great significance. Both the Type 002 and 003 have already begun construction. The Type 003 is expected to include the addition of an electromagnetic aircraft launch system (EMALS)—currently the most advanced aircraft launch system—and nuclear power. If the Type 003 has these features, it will have capabilities similar to the USS Gerald R. Ford—which was commissioned in 2017 as the newest and most advanced U.S. naval carrier. Both the rapid progress of this carrier program and the massive amount of resources devoted to it are evidence of Beijing's intent to become a larger player globally. These carriers will change the operational environment in the near future, create novel challenges in the region, and must be considered when developing short, mid, and long-term strategies regarding China.

That expansion in Chinese naval power would alone make it vital to prioritize a diplomatic approach to managing the changing geopolitical relationship. China's leverage is going to increase as its economy and military continues to grow. Thus, it is in the best interests of the United States to create a deeper and more effective Sino-American dialogue now. This includes negotiating legal agreements before China gets even more leverage. With adequate U.S. influence and pressure in the region, there may be a

[82] United States, Defense Intelligence Agency. (2019, January 3). *China Military Power*. https://www.dia.mil/Portals/27/Documents/News/MilitaryPower/Publications/China_Military_Power_FINAL_5MB_20190103.pdf

possibility for some small agreements regarding arms control and dialogue across multiple domains of great concern and rapid development—including outer space and cyber. Cooperation and dialogue would be in U.S. and neighboring states' best interests. China's growth and goals require some adjustments in the status quo. Outside of the general challenge to the status quo of the international order, some specific Chinese actions are only moderately concerning and are strikingly similar to historical and current paths taken by great Western powers.

China's economic growth and desire to play a more active role in the region has already changed the geopolitical calculus. Some argue that a policy of containment is the proper reaction, but this policy lacks situational awareness and is nearsighted. It is true that the PLA Navy will not achieve complete parity with the U.S. Navy any time soon; however, in a few short years China is expected to achieve technological parity with U.S. Aircraft Carriers and has already developed a fifth-generation fighter—the J-20. A small, but similarly capable, naval fleet in the Indo-Pacific region will substantially change the geopolitical situation and power dynamics. Since the U.S. and other powers are unwilling to go to war with China, by preemptively destroying these already partially built carriers, the U.S. must consider some foreign policy adaptations.

As China continues to become a greater power, the key to achieving long-term peace in Sino-American relations is accepting that Beijing play a larger and more responsible role on terms seen as acceptable and reasonable by the U.S. and its allies. This includes insisting that it become a responsible part of the world order that already exists. It also includes that other countries make reasonable changes that are necessary to account for China's core national security interests. This includes ensuring that the PRC

feels as though it has sovereignty and security. The U.S. should focus its efforts less on fighting China at every point possible and more on setting up an environment favorable to the U.S, while strategically picking its battles. Regarding the South China Sea, negotiations will have concessions on all sides and ultimately create an agreement on which regional actors can agree. However, this does not mean give up or be soft on China. China must and will understand that the U.S. will secure its interests abroad and will defend the freedom of the seas.

Additionally, it is essential that key allies like the Philippines, Taiwan, and others in the region take on a larger role in their defense. The U.S. can and should support these allies, but China must perceive these countries as capable and willing to defend themselves at all costs—instead of perceiving the conflict as being directly with the United States. A focus on ensuring and promoting international support is also essential. Support from the international community will ensure the strength of the international order and create buy-in from other countries. This is also true for recommended actions within the U.S. and through international organizations regarding cyber threats. There are some key issues that both countries will perceive as vital and not easily find compromise on, but the conversations must be had with open minds and dedication.

Stated in the unclassified summary of the 2018 National Defense Strategy, in part "the willingness of rivals to abandon aggression will depend on their perception of U.S. strength and the vitality of our alliances and partnerships".[83] Thus, the U.S. must continue

[83] Mattis, J. (2018, January 19). Summary of the National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

to modernize and build its military capabilities, strengthen international support and alliances—especially with India—and continue to create mutually beneficial economic partnerships. The U.S. must also be willing to make some concessions in areas that are more vital to Chinese national security than U.S. national security.

The amount and type of resources the PRC has dedicated to its military and cyber capacities have made its intentions clear; one way or another China will play a larger role in its region and beyond. This is why creating an environment where China acts more like a partner in the security of the region, instead of an adversary, is absolutely critical. Not only is this shift essential to avoid increased tension and danger, but also can prove to be mutually beneficial. However, work towards this shift needs to begin now. The ability of both sides to view the relationship as more of a partnership is temporally bounded and becomes less likely every day. The stronger the Chinese military and economy get the less Beijing will be willing to negotiate. Additionally, if the countries wait too long to try to accomplish this shift, there likely will be a point of no return and the Sino-U.S. relationship will be so steeped in past transgressions and conflict that a shift in the relationship will become even more difficult, if not impossible.

A Long-term Strategy

China will continue to gain economic, military, and political strength in the Indo-Pacific and abroad. A policy based solely on containment will be counterproductive and fail. Instead, the United States should adopt a policy of rise management as the strategic, long-term goal that accepts the current strategic environment and adapts to the modern

challenges presented by China's rise. Militarily, the U.S. must continue investing and developing to maintain a strong credible deterrent and as much relative strength as possible; this will also maintain a strong position for negotiations. Additionally, the U.S. must be a unifying force and an enable partners and allies to strengthen partnerships and increase defenses to deter aggressive Chinese action.

In the cyber domain, the U.S. must increase defenses and work with the international community to increase capabilities for attribution. The U.S. should clearly convey to Beijing and other actors where it considers cyber-attacks to be escalatory in nature, in order to effectively deter some types of attacks. Economically, the U.S. should be creating and maintaining strong trade and economic partnerships/agreements in the Indo-Pacific. Furthermore, the U.S. should be providing incentives for Beijing to be more involved in current multinational institutions, which may include allowing for Beijing to have greater influence in some decision-making processes. If the U.S. utilizes this policy, managing China's rise will provide the best chance of achieving a long-term peaceful and beneficial U.S. led international order with China acting as a more responsible shareholder.

The Way Forward

In this globalized and rapidly advancing technological world, the national interests of one state are increasingly overlapping with other states' interests. Globalization and the rapid advancement of technology has changed the utility of force in the 21st century. The utility of force has evolved, resulting in a shift in the character of war. This shift entails an increased focus on methods of force mainly below the threshold of traditional armed great power conflict. Furthermore, the actions of one sovereign nation are increasingly likely to impact other sovereign nations. This holds true in many areas, even between states that have different political systems and ideologies. Technology has made the world smaller and significantly increased the ability of actors to cause significant global effects. This is one significant reason why NORAD & USNORTHCOM Commander General O'Shaughnessy states that the "homeland is no longer a sanctuary"[84] and described the situation while testifying before the U.S. Senate Armed Services Committee on 13 February 2020:

> In the years following the Cold War, our nation enjoyed the benefits of military dominance as well as geographic barriers that kept our homeland beyond the reach of most conventional threats… Eroding military advantage is undermining our ability to detect threats, defeat attacks, and therefore deter aggression against the homeland… The threats facing our nations are real and significant. The Arctic

[84] Rempfer, K. (2018, August 27). 'The homeland is no longer a sanctuary' amid rising near-peer threats, NORTHCOM commander says. Retrieved April 25, 2020, from https://www.militarytimes.com/news/your-air-force/2018/08/27/the-homeland-is-no-longer-a-sanctuary-amid-rising-near-peer-threats-northcom-commander-says/

> is no longer a fortress wall, and our oceans are no longer protective moats; they are now avenues of approach for advanced conventional weapons and the platforms that carry them. Our adversaries' capability to directly attack the homeland has leapt forward…[85]

The rapid advance of technology will continue, and new developments of offensive weapons will occur much faster than effective defenses. This demands new strategies and policies, if the U.S. led international order is to thrive. Avoiding severe consequences requires a greater willingness for global cooperation, even between nations and political systems that are vastly different from each other. However, when faced with overtly aggressive actors like Russia, where tensions are already extremely high, the building of defenses as rapidly as possible is critical for defense and deterrence. At the same time, diplomacy, dialogue, and a willingness to respond with strength is essential. The U.S. response to Russian aggression requires more traditional strength through deterrence and strategic messaging, but dialogue and cooperation is still incredibly important for the future of more positive U.S.-Russian relations.

In the cyber domain, the U.S. must increase defenses and work with the international community to increase capabilities for attribution. The U.S. should clearly convey to Beijing, Russia, and other cyber-actors where it considers cyber-attacks to be escalatory in nature, in order to effectively deter. At the same time, innovating and building systems to counter new technological threats is essential. Additionally, the U.S. must build deeper public-private partnerships and enact legislation to increase the protection for the electoral system.

---

[85] Statement of General Terrence J. O'Shaughnessy. (2020, February 13). Retrieved April 25, 2020, from https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-13-20.pdf

China's long-term realist strategy is smart and likely to succeed—barring major events the dramatically shift the geopolitical landscape. It is in the United States best interest to plan for continued Chinese economic growth and influence both regionally and globally. At this point in time, it would be counterproductive, at best, to try to take a hardline containment strategy against China. Instead, the United States can and should take action to create the conditions necessary for Beijing to benefit from becoming a more productive member of the current international order. It is clear that the Communist Party of China does not believe in democracy or freedom. These strong shared values have brought democracies together for decades, but these values will not incentivize China to join the U.S. led liberal order. Instead, Beijing must believe there is actual benefit from being a productive member. Thus, diplomacy and negotiation in terms of economics and power structures will prove of the utmost value. It is essential that the U.S. and other nations be willing to offer actual economic benefits and, in some areas, more authority and responsibility.

The U.S. and its partners must provide incentives and create the necessary conditions for a favorable outcome, but China must ultimately make the decision to take this path forward. In the long-run, small sacrifices today will bring much greater benefits tomorrow. The alternative policy option of using only the stick—attempting to contain China by all means possible—would bring short-term benefits at the cost of long-term disaster. If the Chinese make the wrong choice and threaten the international order that has defended peace and prosperity for decades, then the U.S., its allies, and partner nations must be willing and able to resolutely defeat any and all future threats that may come from China.

The U.S. needs to prioritize efforts to strengthen its economic, political, and military partnerships in the Indo-Pacific. The U.S. must be more involved in economic agreements in the region and place an emphasis on strategic messaging. Until more permanent diplomatic measures are agreed upon, the U.S. must strongly defend the status quo in the SCS and with Taiwan. Additionally, Congress should work towards an Indo-Pacific Deterrence Initiative and the U.S. Senate should ratify the United Nations Convention on the Law of the Sea (UNCLOS). Ratifying UNCLOS will further legitimize U.S. actions in the SCS and the Arctic and decrease perceived U.S. hypocrisy with regard to international rule of law.

The United States must also be keenly aware of growing Sino-Russian relations. Richard Weitz, senior fellow and director of the Center for Political Military analysis at the Hudson Institute, has stated that military ties between these two nations have been growing and:

> "Sino-Russian security cooperation presents challenges to U.S. interests, including to the regional security balance, U.S.-led sanctions, and U.S. military freedom of action and access. These challenges would grow if China and Russia were to form a full-fledged defense alliance."[86]

Weitz says that China and Russia have some mutual interests, especially when it comes to countering the United States and undermining U.S. bilateral and multilateral alliances. He believes that the military ties are set to deepen, which can prove very problematic for

[86] Ellyatt, H. (2019, September 30). Are Russia and China the best of friends now? It's complicated, analysts say. Retrieved May 14, 2020, from https://www.cnbc.com/2019/09/27/russia-and-chinas-relationship--how-deep-does-it-go.html

the United States.[87] If Weitz is correct, the U.S. will need to counter an increase in Sino-U.S. military relations as much as possible and will also need to evaluate what consequence specific actions in the region may have on these relations before taking them.

Globalization, rapid technological advances, and the change in the character of warfare demands new strategies and policies. If the U.S. led international order is to thrive, U.S. policy and strategy must prepare farther into the future than just one four- or eight-year presidential administration. If the United States is to compete effectively with other strategic competitors, longer-term interests need to be of greater importance than short. The U.S. strategy must utilize a whole of government approach to adapt to the modern complex threat environment and keep partisan and policy disputes within manageable limits. Global partnerships must be a priority—and it is essential for the U.S. to be adaptable and dynamic if it is to remain a global leader.

[87] Ellyatt, H. (2019, September 30). Are Russia and China the best of friends now? It's complicated, analysts say. Retrieved May 14, 2020, from https://www.cnbc.com/2019/09/27/russia-and-chinas-relationship--how-deep-does-it-go.html

Afterword: The COVID-19 Pandemic

As this thesis was being finalized, the COVID-19 virus spread across the globe causing the World Health Organization to declare a pandemic.[88] The effects of COVID-19 are expected to be far reaching, although the full impact at this point cannot be known. The global economy will be significantly impacted, at least in the short-term, and the full effects of COVID-19 are yet to be seen as it relates to international relations and geopolitics. "SARS-CoV-2, the virus that causes COVID-19, is thought to have first jumped from an animal host to humans in Wuhan, China"[89] and the full impact this virus will have on the people of China and the Communist Party has also yet to be seen. In March 2020, the Ministry of Foreign Affairs of the People's Republic of China announced that it would be kicking out U.S. journalists during the pandemic.[90] China claimed that this was in reaction to restrictive measures on journalists from China, but removing foreign journalists makes it easier to restrict reporting on the impacts and response to COVID-19 within China. During this critical time and as the situation

[88] Ducharme, J. (2020, March 11). The WHO Just Declared Coronavirus COVID-19 a Pandemic. Retrieved April 26, 2020, from https://time.com/5791661/who-coronavirus-pandemic-declaration/

[89] Ducharme, J. (2020, March 11). The WHO Just Declared Coronavirus COVID-19 a Pandemic. Retrieved April 26, 2020, from https://time.com/5791661/who-coronavirus-pandemic-declaration/

[90] China Takes Countermeasures Against Restrictive Measures on Chinese Media Agencies in the US. (2020, March 18). Retrieved March 19, 2020, from https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1757162.shtml

progresses, the manner in which China-U.S. relations are conducted will likely have an effect on how the foreign policies of both nations evolve. Additionally, there has been a significant drop in oil demand as various types of global stay-at-home orders have been implemented—which will significantly impact Russia, at least in the short-term.

The tragic and deadly COVID-19 pandemic has raised some questions which have yet to be fully answered, especially how it started and what China could or should have done to contain the virus early. Hopefully, the world can learn from this and better prepare for potential future pandemics. Whatever the full impacts may be in China, Russia, and the United States, the consequences of COVID-19 provide additional mutual incentive to try to deepen international dialogue and cooperation in this globalized world, where decisions across the globe can have severe global impacts at home—making everyone a stakeholder.

References

"OSCE Special Monitoring Mission to Ukraine." *OSCE*, www.osce.org/special-monitoring-mission-to-ukraine.

A Europe that protects: EU reports on progress in fighting disinformation ahead of European Council. (2019, June 14). Retrieved April 23, 2020, from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2914

A/RES/73/27 Developments in the field of information and telecommunications in the context of international security. (2018, December 11). Retrieved April 1, 2020, from https://undocs.org/en/A/RES/73/27

Allison, Graham. "The Thucydides Trap: Are the U.S. and China Headed for War?" *The Atlantic*, Atlantic Media Company, 24 Sept. 2015,

Bandow, Doug. "The Ultimate Irony: Is China the 'America' of Asia." *The National Interest*, The Center for the National Interest, 25 Sept. 2016, nationalinterest.org/print/feature/the-ultimate-irony-china-the-america-asia-12976.

Butenko, V., Smith-Spark, L., & Magnay, D. (2014, August 29). U.S. official says 1,000 Russian troops enter Ukraine. Retrieved December 17, 2019, from https://www.cnn.com/2014/08/28/world/europe/ukraine-crisis/index.html.

Chaibong, Hahm. "China's Future Is South Korea's Present." *Foreign Affairs*, vol. 97, no. 5, Sept. 2018.

China Power Team. "What do we know (so far) about China's second aircraft carrier?" China Power. April 22, 2017. Updated May 3, 2019. https://chinapower.csis.org/china-aircraft-carrier-type-001a/

China Takes Countermeasures Against Restrictive Measures on Chinese Media Agencies in the US. (2020, March 18). Retrieved March 19, 2020, from https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1757162.shtml

Chivvis, Christopher S. *Understanding Russian "Hybrid Warfare."* RAND Corporation, 22 Mar. 2017, www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

Coats, D. R. (2019, January 29). *Worldwide Threat Assessment of the US Intelligence Community* (United States, Office of the Director of National Intelligence). https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR-SSCI.pdf

Cronin, Patrick M. "America Must Take a Stand in the South China Sea." *The National Interest*, The Center for the National Interest, 2016, nationalinterest.org/print/feature/america-must-take-stand-the-south-china-sea-13779.

Doffman, Z. (2019, May 6). Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First. https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#53434307afb5

Donaldson, Robert and Nogee, Joseph. The Foreign Policy of Russia. Changing Systems, Enduring Interests. N.Y.: M.E. Sharpe, 2009. – Russia and the Near Abroad. P. 339-376.

Ducharme, J. (2020, March 11). The WHO Just Declared Coronavirus COVID-19 a Pandemic. Retrieved April 26, 2020, from https://time.com/5791661/who-coronavirus-pandemic-declaration/

Dwyer, C. (2018, March 8). The TPP Is Dead. Long Live The Trans-Pacific Trade Deal. Retrieved April 26, 2020, from https://www.npr.org/sections/thetwo-way/2018/03/08/591549744/the-tpp-is-dead-long-live-the-trans-pacific-trade-deal

Ellyatt, H. (2019, September 30). Are Russia and China the best of friends now? It's complicated, analysts say. Retrieved May 14, 2020, from https://www.cnbc.com/2019/09/27/russia-and-chinas-relationship--how-deep-does-it-go.html

Evans, Z. (2019, December 26). U.S. Preparing to Respond to 2020 Russian Election Interference by Releasing Kremlin Officials' Personal Info. Retrieved April 23, 2020, from https://www.nationalreview.com/news/u-s-preparing-to-respond-to-2020-russian-election-interference-by-releasing-kremlin-officials-personal-info/

Garamone, Jim. “New Policy Prohibits GPS Tracking in Deployed Settings.” *U.S. DEPARTMENT OF DEFENSE*, 6 Aug. 2018.

Gramer, R. (2019, June 1). Here's What Russia's Military Build-Up in the Arctic Looks Like. Retrieved April 3, 2020, from https://foreignpolicy.com/2017/01/25/heres-what-russias-military-build-up-in-the-arctic-looks-like-trump-oil-military-high-north-infographic-map/

Groll, E. (2016, October 17). 'Obama's General' Pleads Guilty to Leaking Stuxnet Operation. Retrieved April 1, 2020, from https://foreignpolicy.com/2016/10/17/obamas-general-pleads-guilty-to-leaking-stuxnet-operation/

Heginbotham, E., Nixon, M., Morgan, F. E., Heim, J. L., Hagen, J., Tao Li, S., … Morris, L. J. (2015). An Interactive Look at the U.S.-China Military Scorecard. Retrieved April 28, 2020, from https://www.rand.org/paf/projects/us-china

Johnson, H. (2016, April 18). Why the US Needs to Ratify UNCLOS. Retrieved April 28, 2020, from https://thediplomat.com/2016/04/why-the-us-needs-to-ratify-unclos/

Karber, Phillip. *Russia's 'New Generation Warfare'*. National Geospatial Intelligence Agency, 4 June 2015.

Larsen, Jeffrey Arthur, et al. "NATO's Response to Hybrid Threats." *NATO's Response to Hybrid Threats*, NATO Defense College, 2015.

Majumdar, D. (2016, July 13). Why the United States Needs to Join UNCLOS. Retrieved April 28, 2020, from https://nationalinterest.org/blog/the-buzz/why-the-united-states-needs-join-unclos-16948

Mastro, Oriana Skylar. "The Stealth Superpower." *Foreign Affairs*, Foreign Affairs Magazine, 4 Feb. 2019, www.foreignaffairs.com/articles/china/china-plan-rule-asia.

Mattis, J. (2018, January 19). Summary of the National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National- Defense-Strategy-Summary.pdf

Mizokami, Kyle. “China Could Have 4 Aircraft Carriers by 2022: Should the Navy Be Worried?” *The National Interest*, The Center for the National Interest, 12 Sept. 2018, nationalinterest.org/blog/buzz/china-could-have-4-aircraft-carriers-2022-should-navy-be-worried-31077.

Nadia Diuk. Euromaidan: Ukraine’s Self-Organizing Revolution. April 2014.

NATO. (2020, April 7). Enlargement. Retrieved April 22, 2020, from https://www.nato.int/cps/en/natolive/topics_49212.htm

NATO. (2020, March 30). North Macedonia's flag raised at NATO Headquarters, following accession to NATO. Retrieved April 22, 2020, from https://www.nato.int/cps/en/natohq/news_174648.htm?selectedLocale=en

O'Flaherty, K. (2019, May 08). Israel Retaliates To A Cyber-Attack With Immediate Physical Action In A World First. https://www.forbes.com/sites/kateoflahertyuk/2019/05/06/israel-retaliates-to-a-cyber-attack-with-immediate-physical-action-in-a-world-first/#3251c7b9f895

O’Shaughnessy, Terrence J, et al. “Strategic Shaping: Expanding the Competitive Space.” *Joint Forces Quarterly 90*, 3 July 2018.

Obama, B. (2013, February). *The 2013 State of the Union Address*. Washington D.C.

Office of the Director of National Intelligence. “Assessing Russian Activities and Intentions in Recent US Elections.” *Assessing Russian Activities and Intentions in Recent US Elections*, ODNI, 6 Jan. 2017. www.dni.gov/files/documents/ICA_2017_01.pdf.

Rempfer, K. (2018, August 27). 'The homeland is no longer a sanctuary' amid rising near-peer threats, NORTHCOM commander says. Retrieved April 25, 2020, from

https://www.militarytimes.com/news/your-air-force/2018/08/27/the-homeland-is-no-longer-a-sanctuary-amid-rising-near-peer-threats-northcom-commander-says/

Rosenfeld, E. (2016, July 12). Sweeping ruling against China will have lasting impact globally. Retrieved April 28, 2020, from https://www.cnbc.com/2016/07/12/south-china-sea-breathtaking-ruling-against-china-to-have-lasting-impact.html

Sanger, D. E. (2019). *The Perfect Weapon: War, sabotage, and fear in the cyber age*. New York: Broadway Books.

Sanger, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age / David E. Sanger.* First ed., 2018.

Sarbanes, J. P. (2019, March 14). Text - H.R.1 - 116th Congress (2019-2020): For the People Act of 2019. Retrieved April 23, 2020, from https://www.congress.gov/bill/116th-congress/house-bill/1/text#

Schreck, C. (2019, February 26). From 'Not Us' To 'Why Hide It?': How Russia Denied Its Crimea Invasion, Then Admitted It. Retrieved December 17, 2019, from https://www.rferl.org/a/from-not-us-to-why-hide-it-how-russia-denied-its-crimea-invasion-then-admitted-it/29791806.html.

Silver, C. (2020, April 17). The Top 20 Economies in the World. Retrieved April 28, 2020, from https://www.investopedia.com/insights/worlds-top-economies/

Snyder, Timothy. *The Road to Unfreedom: Russia, Europe, America*. First ed., 2018.

Statement of General Terrence J. O'Shaughnessy Before the House Armed Services Committee Subcommittee on Strategic Forces. Terrence, O. S. J. (2020, March 12). Retrieved April 22, 2020, from

https://docs.house.gov/meetings/AS/AS29/20200312/110671/HHRG-116-AS29-Wstate-OShaughnessyT-20200312.pdf

Statement of General Terrence J. O'Shaughnessy Before the Senate Armed Services Committee. (2020, February 13). Retrieved April 25, 2020, from https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-13-20.pdf

Territorial Disputes in the South China Sea | Global Conflict Tracker. (2019, May 31). Retrieved from https://www.cfr.org/interactive/global-conflict-tracker/conflict/territorial-disputes-south-china-sea

The Role of Regional Organizations in Strengthening Cybersecurity and Stability. (2019, January 24). Retrieved April 1, 2020, from https://www.unidir.org/publication/role-regional-organizations-strengthening-cybersecurity-and-stability

Thornberry Unveils Indo-Pacific Deterrence Initiative. (2020, April 16). Retrieved May 19, 2020, from https://republicans-armedservices.house.gov/news/press-releases/thornberry-unveils-indo-pacific-deterrence-initiative

United States, Defense Intelligence Agency. (2019, January 3). *China Military Power*. Retrieved April 16, 2019, from https://www.dia.mil/Portals/27/Documents/News/Military Power Publications/China_Military_Power_FINAL_5MB_20190103.pdf

United States, Office of the President. "National Cyber Strategy of the United States of America." *National Cyber Strategy of the United States of America*, The White House, 2018.

United States, The White House. (2017, December). *National Security Strategy of the United States of America*. Retrieved April 16, 2019, from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

U.S. Relations With Taiwan - United States Department of State. (2020, February 13). Retrieved May 14, 2020, from https://www.state.gov/u-s-relations-with-taiwan/

Walt, S. M. (2017, May 3). This Isn't Realpolitik. This Is Amateur Hour. Retrieved April 26, 2020, from https://foreignpolicy.com/2017/05/03/this-isnt-realpolitik-this-is-amateur-hour/

World Bank. (n.d.). Data for China, United States . Retrieved April 28, 2020, from https://data.worldbank.org/?locations=CN-US

Yuhas, Alan, and Raya Jalabi. "Ukraine Crisis: Why Russia Sees Crimea as Its Naval Stronghold." *The Guardian*. 7 Mar. 2014.

Appendix

China's Territorial Claims

91

[91] United States, Defense Intelligence Agency. (2019, January 3). *China Military Power*. Retrieved April 16, 2019, from https://www.dia.mil/Portals/27/Documents/News/Military Power Publications/China_Military_Power_FINAL_5MB_20190103.pdf